ID: 553989
Sample Name:
Frkmlkdkdubkznbkmcf.dll
Cookbook: default.jbs
Time: 02:35:22
Date: 17/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Frkmlkdkdubkznbkmcf.dll 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Initial Sample 3
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 4
AV Detection: 4
System Summary: 4
Data Obfuscation: 4
HIPS / PFW / Operating System Protection Evasion: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
Contacted IPs 7
General Information 7
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 8
General 8
File Icon 8
Static PE Info 9
General 9
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 9
Imports 9
Version Infos 9
Network Behavior 9
Code Manipulations 9
Statistics 9
Behavior 9
System Behavior 10
Analysis Process: loaddll32.exe PID: 6088 Parent PID: 4964 10
General 10
File Activities 10
Analysis Process: cmd.exe PID: 5696 Parent PID: 6088 10
General 10
File Activities 10
Analysis Process: rundll32.exe PID: 2008 Parent PID: 5696 10
General 10
File Activities 11
Disassembly 11
Code Analysis 11

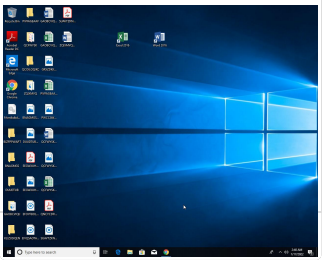
Windows Analysis Report Frkmlkdkdubkznbkmcf.dll

Overview

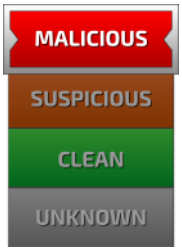
General Information

Sample Name:	Frkmlkdkdubkznbkmcf.dll
Analysis ID:	553989
MD5:	e61518ae9454a5..
SHA1:	82d29b52e35e79..
SHA256:	9ef7dbd3da51332.
Tags:	dll WhisperGate
Infos:	

Most interesting Screenshot:



Detection

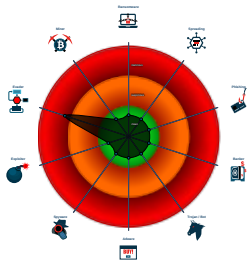


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Call by …
- .NET source code contains potentia…
- .NET source code references suspic…
- Yara signature match
- Program does not show much activi…
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6088 cmdline: loaddll32.exe "C:\Users\user\Desktop\Frkmlkdkdubkznbkmcf.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5696 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Frkmlkdkdubkznbkmcf.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 2008 cmdline: rundll32.exe "C:\Users\user\Desktop\Frkmlkdkdubkznbkmcf.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Frkmlkdkdubkznbkmcf.dll	MAL_OBFUSC_Unknown_Jan22_1	Detects samples similar to reversed stage3 found in Ukrainian wiper incident named WhisperGate	Florian Roth	• 0x43da8:$xc1: 37 00 63 00 38 00 63 00 62 00 35 00 35 00 39 00 38 00 65 00 37 00 32 00 34 00 64 00 33 00 34 00 33 00 38 00 34 00 63 00 63 00 65 00 37 00 34 00 30 00 32 00 62 00 31 00 31 00 66 00 30 00 65 • 0x3ff6e:$xc2: 4D 61 69 6E 00 43 6C 61 73 73 4C 69 62 72 61 72 79 31 00 70 63 31 65 • 0x44216:$s1: .dll • 0x442c2:$s1: .dll • 0x3e471:$s2: %&%,%s% • 0x2fed8:$op1: A2 87 FA B1 44 A5 F5 12 DA A7 49 11 5 C 8C 26 D4 75 • 0x26d5f:$op2: D7 AF 52 38 C7 47 95 C8 0E 88 F3 D5 0B • 0x1f499:$op3: 6C 05 DF D6 B8 AC 11 F2 67 16 CB B7 34 4D B6 91

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Data Obfuscation:

.NET source code contains potential unpacker

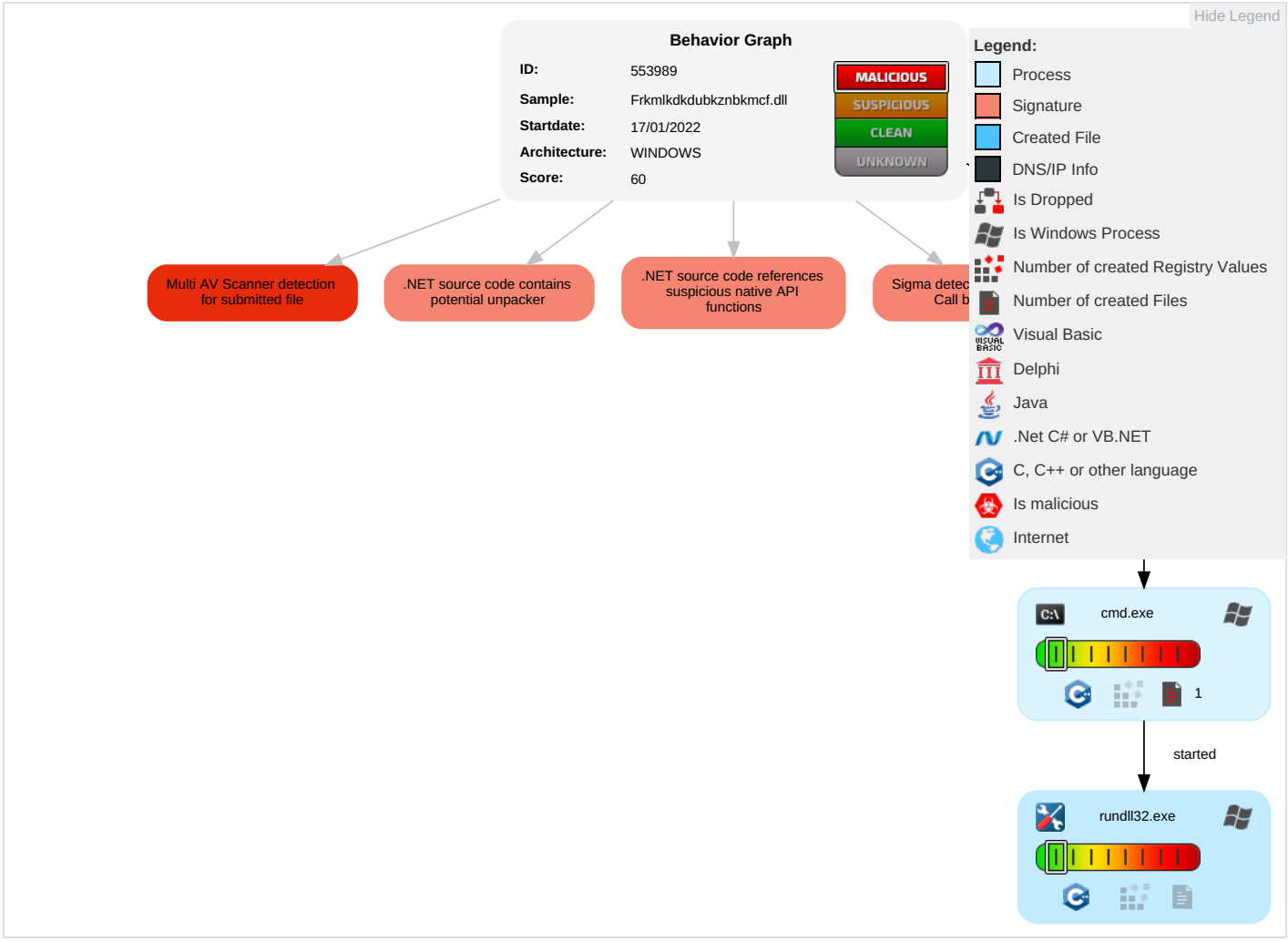
HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Native API 1	Path Interception	Process Injection 1 1	Rundll32 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	F T V A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	F V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	C D C E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

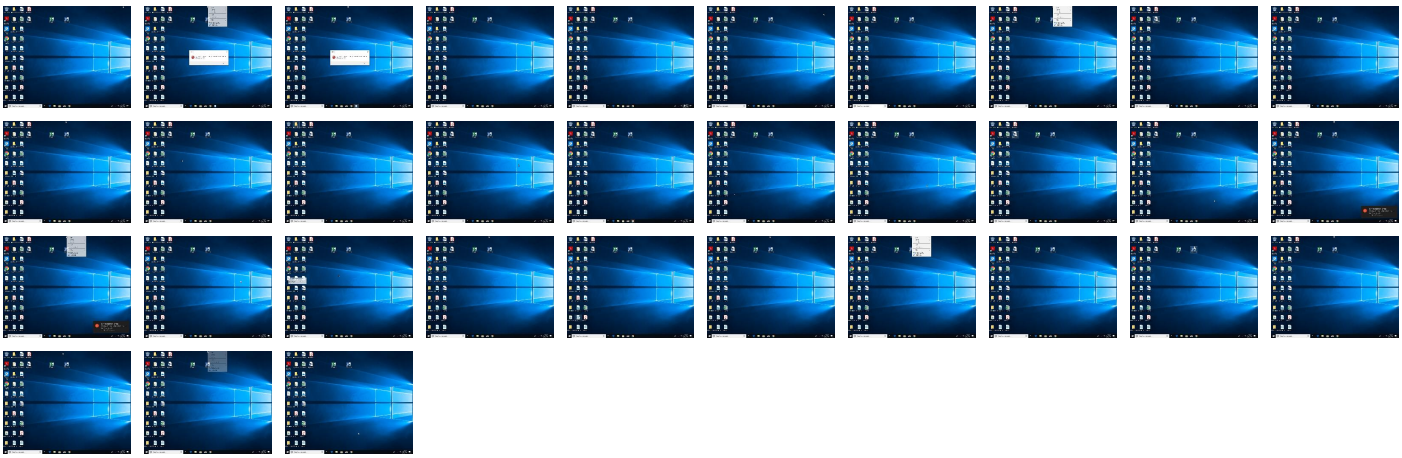
Behavior Graph



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
Frkmlkdkdubkznbkmcf.dll	16%	Virustotal		Browse
Frkmlkdkdubkznbkmcf.dll	8%	Metadefender		Browse
Frkmlkdkdubkznbkmcf.dll	23%	ReversingLabs	Win32.Network.WhisperGate	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553989
Start date:	17.01.2022
Start time:	02:35:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Frkmlkdkdubkznbkmcf.dll
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:	26
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:	mal60.evad.winDLL@5/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
02:36:14	API Interceptor	1x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.916354202479544
TrID:	• Win32 Dynamic Link Library (generic) Net Framework (1011504/3) 50.14% • Win32 Dynamic Link Library (generic) (1002004/3) 49.67% • Generic Win/DOS Executable (2004/3) 0.10% • DOS Executable Generic (2002/1) 0.10% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Frkmlkdkdubkznbkmcf.dll
File size:	280064
MD5:	e61518ae9454a563b8f842286bbdb87b
SHA1:	82d29b52e35e7938e7ee610c04ea9daaf5e08e90
SHA256:	9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
SHA512:	7a30af55518eb2f125ad475b3e495b9beebcc7cba2adf5d9edf3aa1a9e0a351b53df430061089cdcebe3073364754ccad4d2ca22b05c84c925089a0229f04e6e
SSDEEP:	6144:i9JxgDyGljt5zFSb4rKWFV1y3QXJgGsHYjohn/wkKLwZl8UYrOqvM:irxgDyGljt5zF9xS2j8Km4kYM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#E.a..... .....>.....]... ...`....@.. .....@.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x445da6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61DC4523 [Mon Jan 10 14:39:31 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	dae02f32a21e03ce65412f6e56942daa

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x43dac	0x43e00	False	0.631226260359	data	6.9383493763	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x35c	0x400	False	0.345703125	data	2.69926905034	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x48000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6088 Parent PID: 4964

General

Start time:	02:36:13
Start date:	17/01/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\FrkmlkdkdubkznbkmcF.dll"
Imagebase:	0x50000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5696 Parent PID: 6088

General

Start time:	02:36:13
Start date:	17/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\FrkmlkdkdubkznbkmcF.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 2008 Parent PID: 5696

General

Start time:	02:36:14
Start date:	17/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\FrkmlkdkdubkznbkmcF.dll",#1
Imagebase:	0x90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis