

JoeSandbox Cloud BASIC



ID: 546181

Sample Name:

OfficialKiddionsModMenuV0.8.7.exe

Cookbook: default.jbs

Time: 08:50:28

Date: 29/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report OfficialKiddionsModMenuV0.8.7.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: RedLine	4
Yara Overview	4
PCAP (Network Traffic)	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
System Summary:	5
Hooking and other Techniques for Hiding and Protection:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Stealing of Sensitive Information:	5
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	11
General	11
File Icon	11
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	12
Sections	12
Resources	12
Imports	12
Possible Origin	12
Network Behavior	13
Network Port Distribution	13
TCP Packets	13
Code Manipulations	13
Statistics	13
Behavior	13
System Behavior	13
Analysis Process: OfficialKiddionsModMenuV0.8.7.exe PID: 7072 Parent PID: 3608	13
General	13
Analysis Process: AppLaunch.exe PID: 6652 Parent PID: 7072	13
General	14
File Activities	14
File Created	14
File Written	14
File Read	14

Disassembly	14
Code Analysis	14

Windows Analysis Report OfficialKiddionsModMenuV0....

Overview

General Information

Sample Name:	OfficialKiddionsModMenuV0.8.7.exe
Analysis ID:	546181
MD5:	7de3896baf12500.
SHA1:	500b906981aaa4..
SHA256:	213fce24e326925.
Tags:	exe
Infos:	
Most interesting Screenshot:	

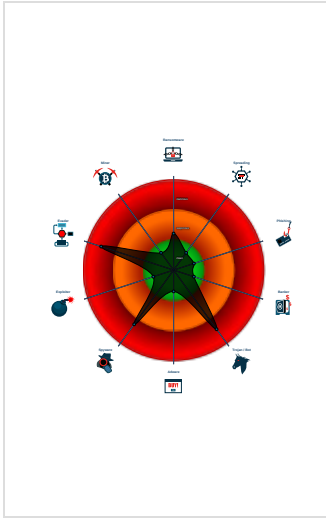
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>RedLine</div>	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Yara detected RedLine Stealer
Found malware configuration
Multi AV Scanner detection for subm...
Overwrites code with unconditional j...
Writes to foreign memory regions
Tries to shutdown other security too...
Tries to steal Crypto Currency Wallets
Tries to detect sandboxes and other...
Machine Learning detection for samp...
Allocates memory in foreign process...
Injects a PE file into a foreign proce...
Queries sensitive video device inform...

Classification



Process Tree

System is w10x64
<ul style="list-style-type: none"> OfficialKiddionsModMenuV0.8.7.exe (PID: 7072 cmdline: "C:\Users\user\Desktop\OfficialKiddionsModMenuV0.8.7.exe" MD5: 7DE3896BAF12500F3E1CD311E2340806)<ul style="list-style-type: none"> AppLaunch.exe (PID: 6652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
cleanup

Malware Configuration

Threatname: RedLine

{ "C2_url": "103.246.144.29:44301" }

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.292031662.000000000000C 2000.00000004.00000001.sdump	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000000A.00000002.348909899.0000000000040 2000.00000020.00000001.sdump	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000003.291666157.00000000003B1 2000.00000040.00000001.sdump	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: AppLaunch.exe PID: 6652	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	


Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.OfficialKiddionsModMenuV0.8.7.exe.c3b54.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
10.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.3.OfficialKiddionsModMenuV0.8.7.exe.3b10000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:



PE file has nameless sections

Hooking and other Techniques for Hiding and Protection:



Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion:



Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:



Writes to foreign memory regions

Tries to shutdown other security tools via broadcasted WM_QUERYENDSESSION

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Tries to harvest and steal browser information (history, passwords, etc)

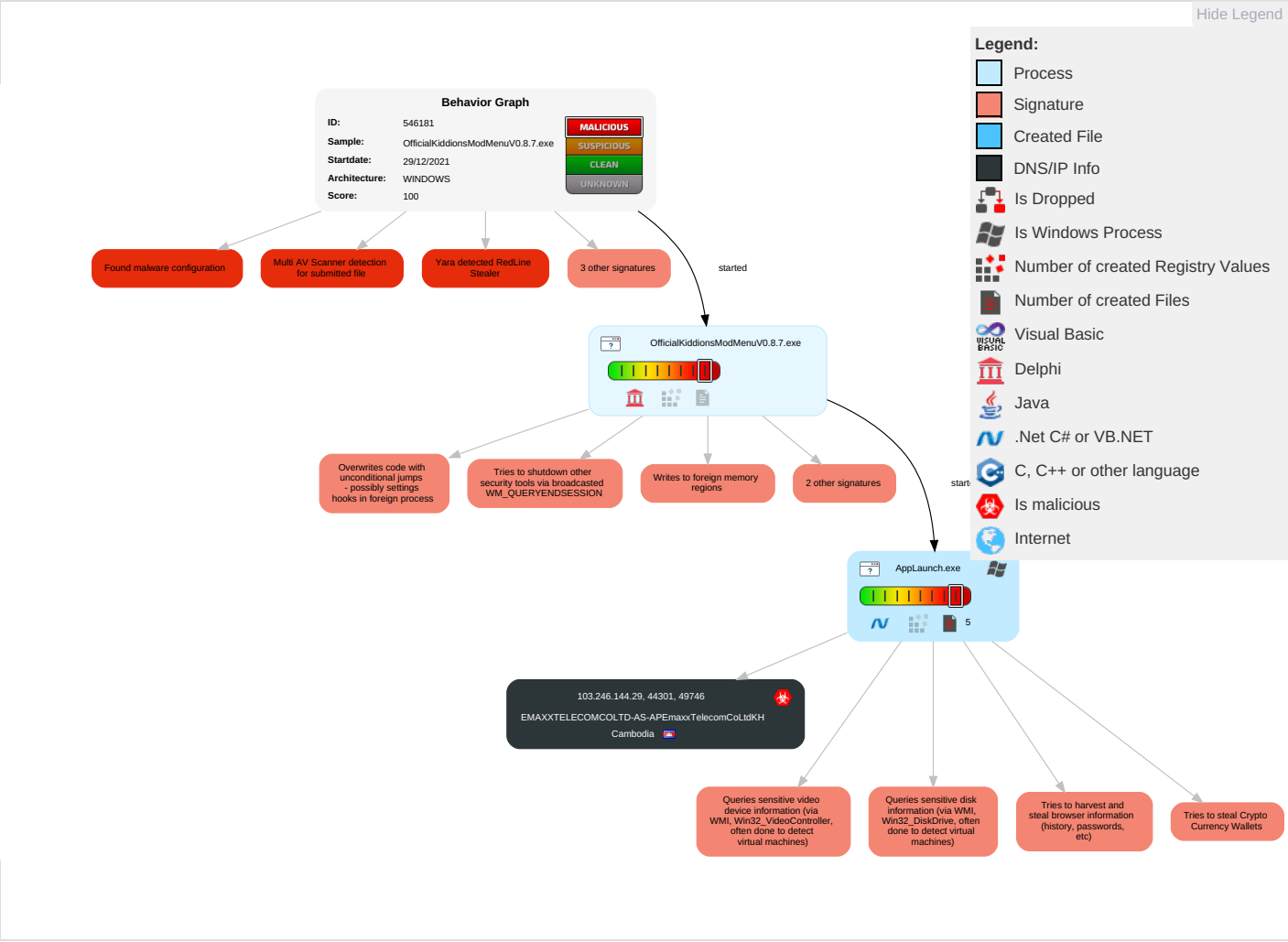


Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 3 1 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	Credential API Hooking 1	Process Discovery 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Input Capture 1	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
OfficialKiddionsModMenuV0.8.7.exe	26%	Virustotal		Browse
OfficialKiddionsModMenuV0.8.7.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.OfficialKiddionsModMenuV0.8.7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.OfficialKiddionsModMenuV0.8.7.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.OfficialKiddionsModMenuV0.8.7.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.246.144.29	unknown	Cambodia		58447	EMAXXTELECOMCOLTD-AS-APEmaxxTelecomCoLtdKH	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	546181
Start date:	29.12.2021
Start time:	08:50:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OfficialKiddionsModMenuV0.8.7.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@0/1
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 88.1% (good quality ratio 73.8%)• Quality average: 64.2%• Quality standard deviation: 34.1%
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 87%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:51:51	API Interceptor	17x Sleep call for process: AppLaunch.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

C:\Users\user1\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKHqNoPtHoxHlmHKAHK1HxLHG1qHqH5HX: vq5qXAqLqdqUqzcGYqhQnoPtXhBqAqG
MD5:	174E563C986AB09114A6F31F870A6E13
SHA1:	F68EFD04D0559B24C448E629A0115F2E6C3B39D
SHA-256:	465C8001CEFD747AF8A94EDD62CC829D8DFF4D6BED174591DA0B71E10FDC584F
SHA-512:	252A2B615BB7BB4223F0873F41CC7C4BC6576172CD704DD93926E004CD5795CA5DC2DE3332586BF3C44E0B564148A7661563C00B204649C7A5594C097C1E9EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\B219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.999073227693366
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.96%Generic Win/DOS Executable (2004/3) 0.02%DOS Executable Generic (2002/1) 0.02%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	OfficialKiddionsModMenuV0.8.7.exe
File size:	4397056
MD5:	7de3896baf12500f3e1cd311e2340806
SHA1:	500b906981aaa4810848643f1d8c17efa87bad20
SHA256:	213fce24e326925749adebaff2d85e23bba2b616c872e2089b23fa231f18756e
SHA512:	d08cf4dcb3170f4654ef7121078b2c902285732dc3b2292d1a1e9d576f639050c98c08e8d1391b1bfa46f313bb9b8840968b86077d5e52f49e882994f13abef1
SSDEEP:	98304:xAM03cGX50EXFEACRwiGbJ3hjOQxsaS3XnLUBzEydzEI:xBM03c+0ACRZGNBdONX5
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode.....\$.PE..L....a.a.....@.....@.....n.....C.....

File Icon



Icon Hash:	00828e8e8686b000
------------	------------------

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x61CB6117 [Tue Dec 28 19:10:15 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	9a4258c5d218cf6e5c500e8415d5f5ed

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x22000	0x11400	False	1.00043874547	data	7.99788481833	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x23000	0x47c	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x24000	0xf000	0x7a00	False	1.00051229508	data	7.9951936828	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x33000	0x2000	0x400	False	1.0107421875	data	7.79914503297	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x35000	0x26c1d5	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x2a2000	0x3fb000	0x3cd400	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x69d000	0x1000	0x200	False	0.9453125	data	6.95928882324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.yke1AWY	0x69e000	0x4b000	0x4ac00	False	0.98668412939	data	7.91755317496	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x6e9000	0x1000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior


Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: OfficialKiddionsModMenuV0.8.7.exe PID: 7072 Parent PID: 3608

General

Start time:	08:51:22
Start date:	29/12/2021
Path:	C:\Users\user\Desktop\OfficialKiddionsModMenuV0.8.7.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\OfficialKiddionsModMenuV0.8.7.exe"
Imagebase:	0x400000
File size:	4397056 bytes
MD5 hash:	7DE3896BAF12500F3E1CD311E2340806
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.292031662.00000000000C2000.00000004.00000001.sdmp, Author: Joe SecurityRule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000003.291666157.0000000003B12000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: AppLaunch.exe PID: 6652 Parent PID: 7072

General

Start time:	08:51:26
Start date:	29/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Applaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Applaunch.exe
Imagebase:	0x2b0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000A.00000002.348909899.0000000000402000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis