ID: 435329
Sample Name:
gmAszjZqKD.exe
Cookbook: default.jbs
Time: 12:28:08
Date: 16/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Windows Analysis Report gmAszjZqKD.exe

Overview

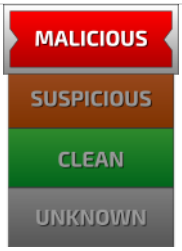
General Information

Sample Name:	gmAszjZqKD.exe
Analysis ID:	435329
MD5:	a8fcf9f01f6ac912..
SHA1:	40072436d5bd26..
SHA256:	9d56ad7e390d35..
Tags:	AveMariaRAT exe RAT
Infos:	

Errors

- Nothing to analyse, Joe Sandbox has not found any analysis process or sample
- Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

Detection



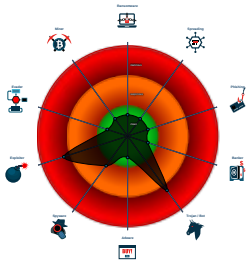
AveMaria UACMe

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AveMaria stealer
- Yara detected UACMe UAC Bypass…
- Contains functionality to hide user a…
- Machine Learning detection for samp…
- Installs a raw input device (often for …
- PE file contains executable resource…
- PE file overlay found
- Uses 32bit PE files
- Yara detected Credential Stealer

Classification



Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
gmAszjZqKD.exe	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
gmAszjZqKD.exe	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	• 0x191f0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x191f0:$c1: Elevation:Administrator!new:
gmAszjZqKD.exe	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x144e8:$a1: \Opera Software\Opera Stable\Login Data • 0x14810:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14158:$a3: \Google\Chrome\User Data\Default\Login Data
gmAszjZqKD.exe	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
gmAszjZqKD.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 2 entries

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Yara detected AveMaria stealer
- Machine Learning detection for sample

Exploits:

- Yara detected UACMe UAC Bypass tool

E-Banking Fraud:

- Yara detected AveMaria stealer

System Summary:

- Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

- Contains functionality to hide user accounts

Stealing of Sensitive Information:

- Yara detected AveMaria stealer

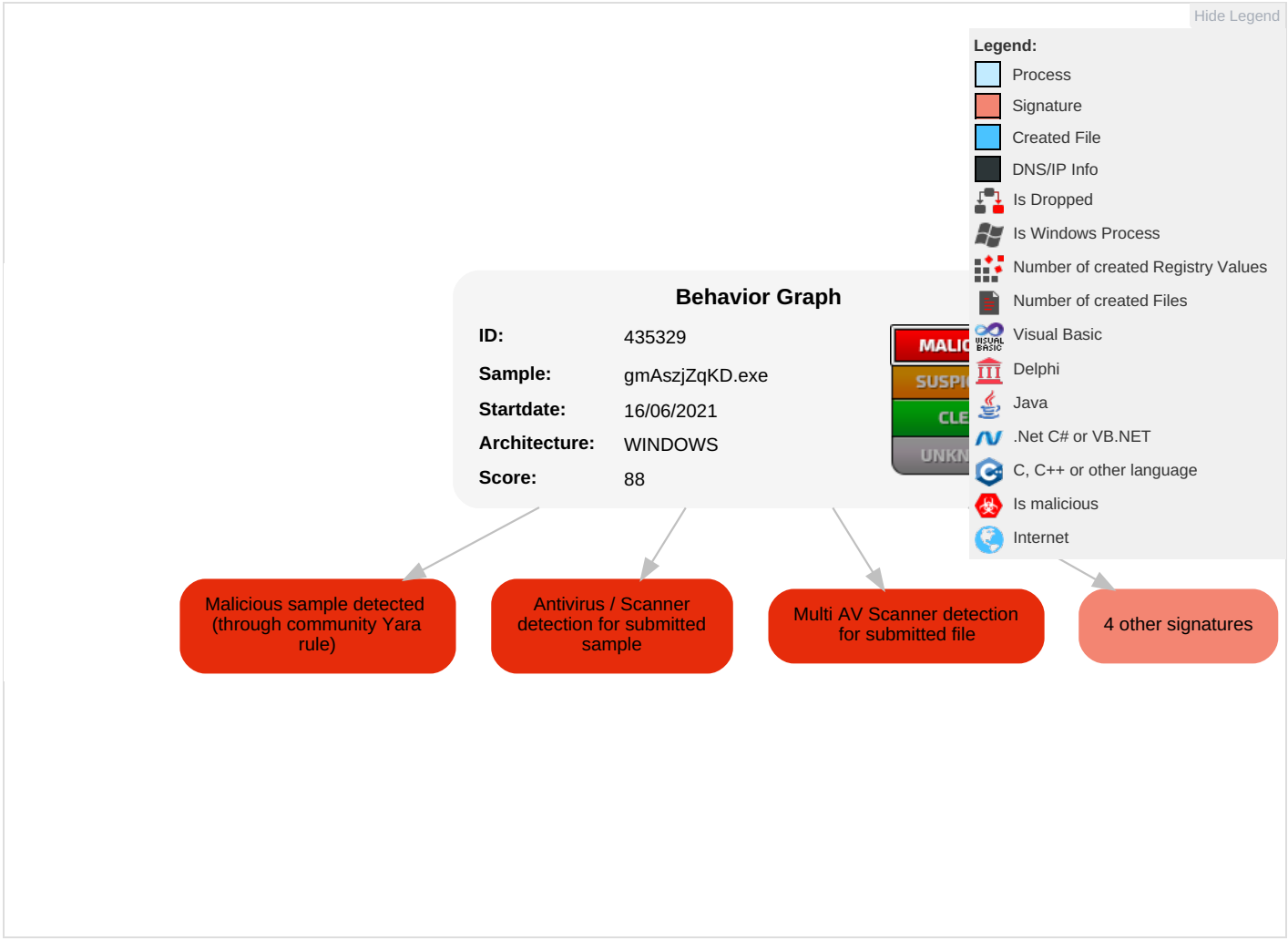
Remote Access Functionality:

- Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Hidden Users 1	Input Capture 1 1	System Service Discovery	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
gmAszjZqKD.exe	72%	Virustotal		Browse
gmAszjZqKD.exe	90%	ReversingLabs	Win32.Backdoor.Remcos	
gmAszjZqKD.exe	100%	Avira	TR/Redcap.ghjpt	
gmAszjZqKD.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	435329
Start date:	16.06.2021
Start time:	12:28:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	gmAszjZqKD.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:	3
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:	mal88.troj.expl.winEXE@0/0@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Unable to launch sample, stop analysis
Warnings:	Show All
Errors:	• Nothing to analyse, Joe Sandbox has not found any analysis process or sample • Corrupt sample or wrongly selected analyzer. Details: %1 is not a valid Win32 application.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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):	6.3223585086508205
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:	gmAszjZqKD.exe
File size:	112035
MD5:	a8fcf9f01f6ac912a38cb17e59eb1ed0
SHA1:	40072436d5bd265261bcf0bfd5cfbb046e70a97a
SHA256:	9d56ad7e390d35d3fcf2bc03ac7b38e5efeee12e8bbc2917a375e6cf8c65d69f
SHA512:	e59eb3818a70cb1fbf3b0463622faec08320109d1791aaf7c7052ecd1dfec3ed1c7e645aa54f02f773367989b2f6031e8b1962fd548ff7ef00e8e4475d26005d
SSDEEP:	1536:h0jP7/L1B5rVmN8sxHv2M28ix8EUaJxWZoB4u0OVE013:K1VmhaH8EFvW+0OVE0h
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z]..><..><..><...3..?<..7D..?<...3..<<.....?<.....=<..;0..?<..7D..:<..7D..!<..><...<...U..N<...Um.?<...U..?<..Rich><.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x405ce2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F49FB9C [Sat Aug 29 06:54:20 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	51a1d638436da72d7fa5fb524e02d427

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12eab	0x13000	False	0.574822676809	data	6.49494739154	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x14000	0x49ce	0x4a00	False	0.404666385135	data	5.28154165346	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x19000	0x1350d8	0x600	False	0.570963541667	data	4.99296329391	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14f000	0x2c70	0x2e00	False	0.327785326087	data	3.95871566709	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x152000	0xfa8	0x1000	False	0.926960257787	data	6.58382237931	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.bss	0x153000	0x1000	0x200	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	India	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Disassembly