

JOeSandbox Cloud BASIC



ID: 431849

Sample Name: dt9XEhpeQQ

Cookbook: default.jbs

Time: 12:54:54

Date: 09/06/2021

Version: 32.0.0 Black Diamond




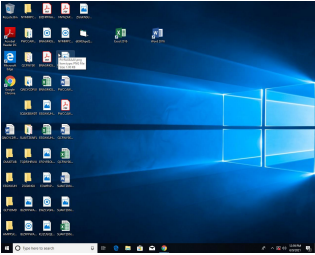
Table of Contents

Table of Contents	2
Analysis Report dt9XEhpeQQ	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: dt9XEhpeQQ.exe PID: 3924 Parent PID: 5716	10
General	10
Disassembly	10
Code Analysis	10

Analysis Report dt9XEhpeQQ

Overview

General Information

Sample Name:	dt9XEhpeQQ (renamed file extension from none to exe)
Analysis ID:	431849
MD5:	5423976b486afd6.
SHA1:	f04947aa1b4e950.
SHA256:	e73ecaf549049b8.
Infos:	  
Most interesting Screenshot:	
	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Potential malicious icon found

Yara detected GuLoader

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

Machine Learning detection for samp...

Tries to detect virtualization through...

Abnormal high CPU Usage

Contains functionality for execution ...

Contains functionality to call native f...


Contains functionality to read the PEB

Detected potential crypto function

Classification



Process Tree

- System is w10x64
-  dt9XEhpeQQ.exe (PID: 3924 cmdline: 'C:\Users\user\Desktop\dt9XEhpeQQ.exe' MD5: 5423976B486AFD6A8DAD047FB947B190)
- cleanup

Malware Configuration

No configs have been found

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.726927827.0000000000227 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

 Click to jump to signature section

AV Detection:



Machine Learning detection for sample

System Summary:



Potential malicious icon found

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 virtualization through RDTSC time measurements

Anti Debugging:

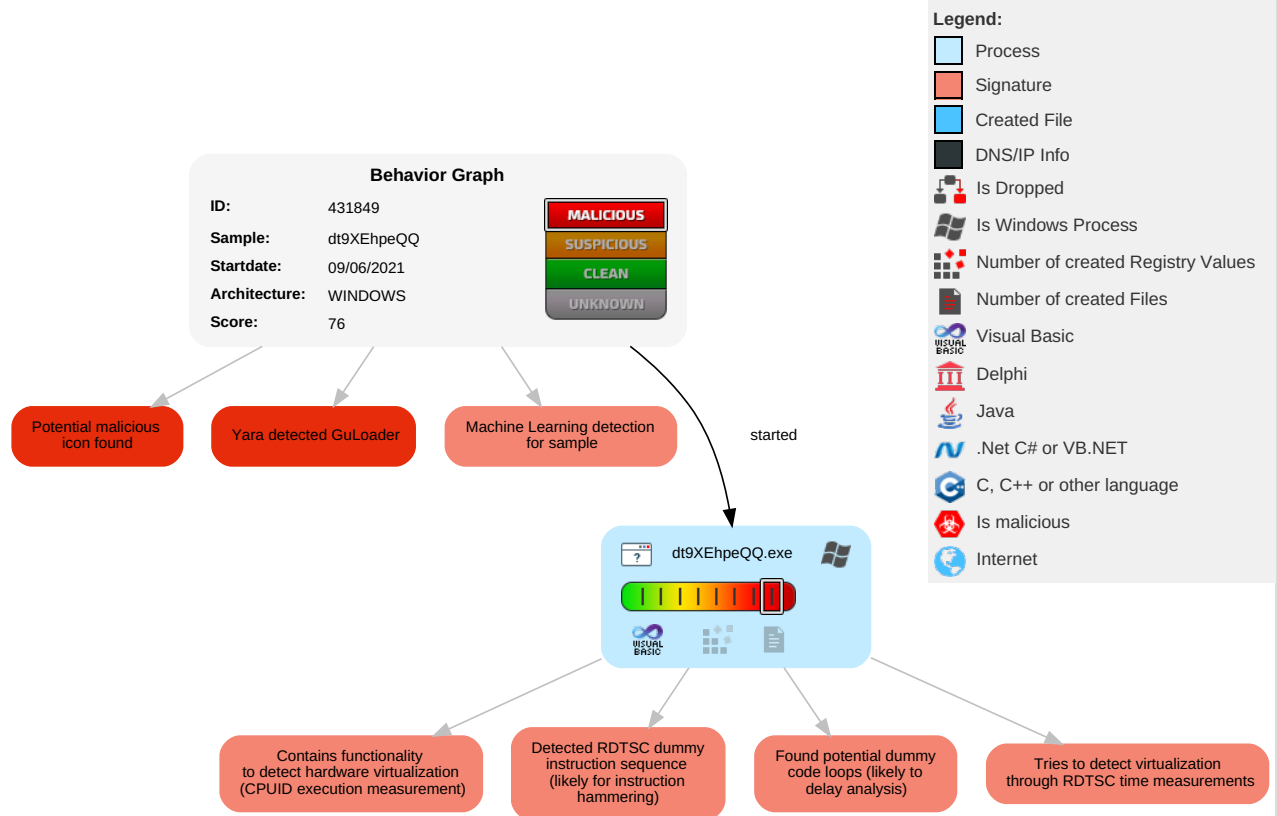


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

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
dt9XEhpeQQ.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431849
Start date:	09.06.2021
Start time:	12:54:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dt9XEhpeQQ (renamed file extension from none to 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:	36
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 0.3% (good quality ratio 0.3%)• Quality average: 50.2%• Quality standard deviation: 2.2%
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 52%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• 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

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):	3.8630055260118947
TrID:	<ul style="list-style-type: none">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:	dt9XEhpeQQ.exe
File size:	204800
MD5:	5423976b486afd6a8dad047fb947b190
SHA1:	f04947aa1b4e9500e4b31d2365ac886447ba4427
SHA256:	e73ecaf549049b8c4f8701e55c95220e09890df2d93ef52465ccd4b448a6d19f
SHA512:	8b4e3e0110d9a24efc2b4fd4ba79bc9aa5dfedb0d567259cd7068d361d7a1f85bfb55dca921700bb90faf3ade1820ce87b6b8e60f9436dff0b90780e084b1dd6
SSDEEP:	1536:9hWwhz1JjHnmEik/dZNgmZZfOc7Gec1GvI5wumCWC0tkC:+whR/dZNgmz2Qq1GUwumCWC0tV
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode.....\$......U...1...1..1.....0...~...0.....0...Rich1.....PE..L....4DK.....@.....h.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x401368
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:	0x4B443402 [Wed Jan 6 06:56:02 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:	b2e3727c442d471988cc35e3702b319a

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2e6ec	0x2f000	False	0.229549326795	data	3.95505433936	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x30000	0xa7c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0x994	0x1000	False	0.17919921875	data	2.11718629693	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

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: dt9XEhpeQQ.exe PID: 3924 Parent PID: 5716

General

Start time:	12:55:39
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\dt9XEhpeQQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dt9XEhpeQQ.exe'
Imagebase:	0x400000
File size:	204800 bytes
MD5 hash:	5423976B486AFD6A8DAD047FB947B190
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.726927827.0000000002270000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis