ID: 357952
Sample Name:
OPDATERINGSDISKETTES.exe
Cookbook: default.jbs
Time: 01:14:59
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

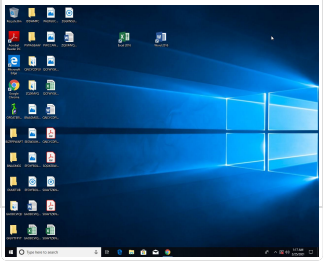
Analysis Report OPDATERINGSDISKETTES.exe

Overview

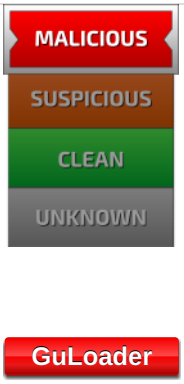
General Information

Sample Name:	OPDATERINGSDISKETTES.exe
Analysis ID:	357952
MD5:	446701e67dd00e..
SHA1:	1acbd6fae421f3c..
SHA256:	2414764b6c9385..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



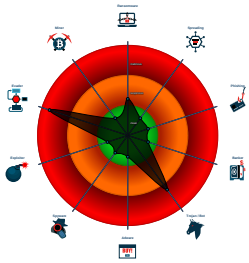
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- OPDATERINGSDISKETTES.exe (PID: 4316 cmdline: 'C:\Users\user\Desktop\OPDATERINGSDISKETTES.exe' MD5: 446701E67DD00E1D2C45B23263533DEA)
  - RegAsm.exe (PID: 1948 cmdline: 'C:\Users\user\Desktop\OPDATERINGSDISKETTES.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

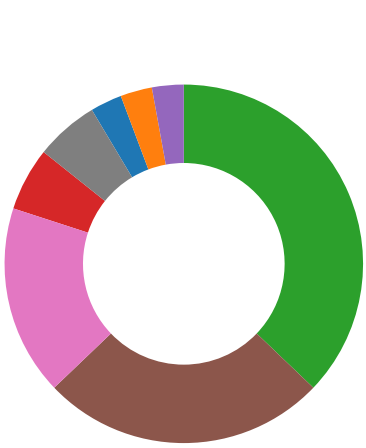
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 1948	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

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 Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

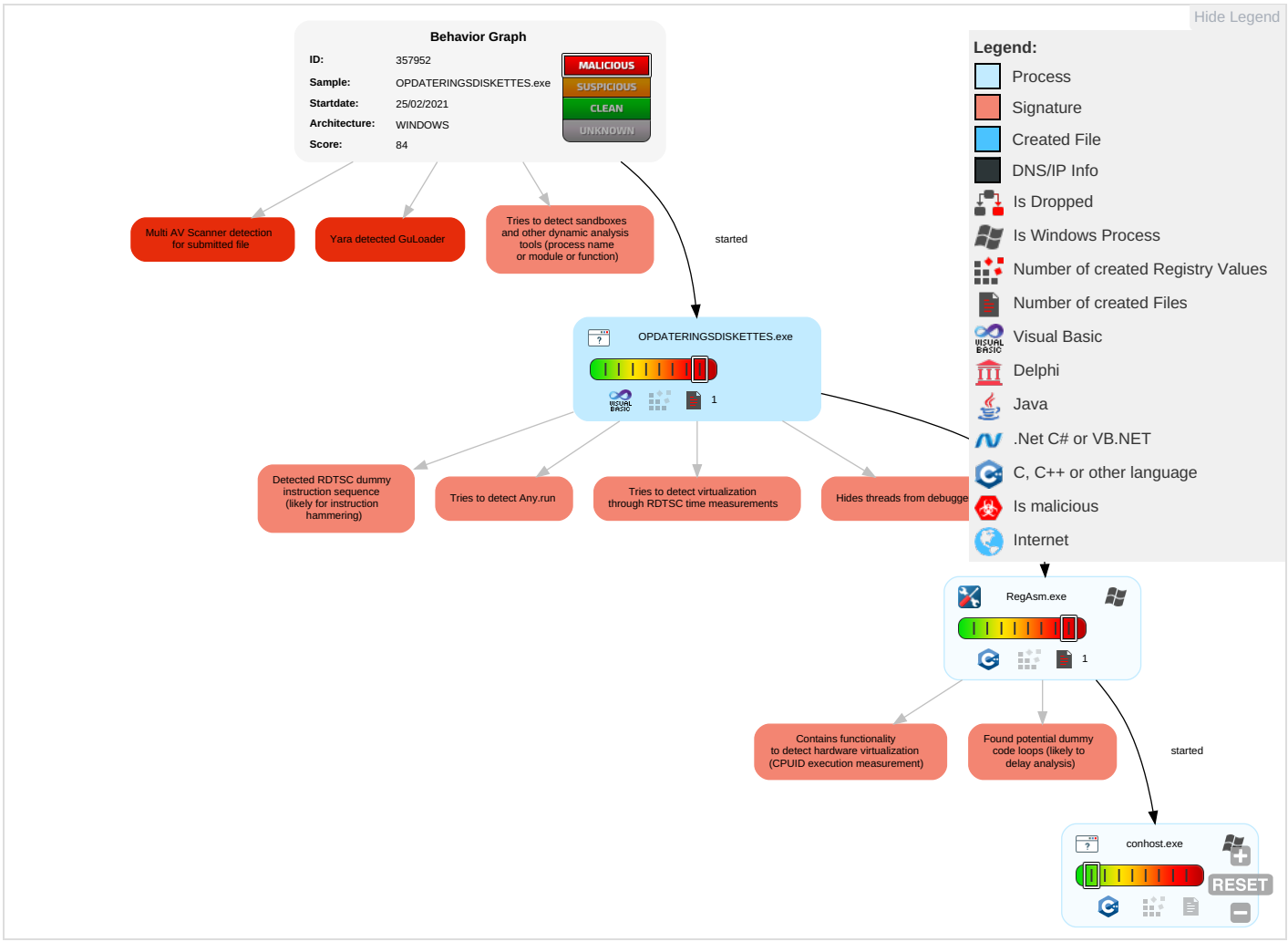
Hides threads from debuggers

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	DLL Side-Loading 1	Process Injection 1 2	Virtualization/Sandbox Evasion 3 1 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

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
OPDATERINGSDISKETTES.exe	21%	Virustotal		Browse
OPDATERINGSDISKETTES.exe	11%	ReversingLabs	Win32.Worm.Wbvb	

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:	31.0.0 Emerald
Analysis ID:	357952
Start date:	25.02.2021
Start time:	01:14:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OPDATERINGSDISKETTES.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:	23
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:	mal84.troj.evad.winEXE@4/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 94% (good quality ratio 56%) • Quality average: 40.7% • Quality standard deviation: 38%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe

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):	5.4029031708300606
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:	OPDATERINGSDISKETTES.exe
File size:	73728
MD5:	446701e67dd00e1d2c45b23263533dea
SHA1:	1acbd6fae421f3cc96e757138c9af9e4fc5b5d3a
SHA256:	2414764b6c9385725e8ad59646c7af513fe3cd1bdd0de671dea8dc04ba4c6fe3
SHA512:	fccf60e2acc13f6be8f9bb5644bc5d7f6e62a39ff08ec6d75c6016677924cf91cf26be59f7952a16bfb7c750f083225ba26034cf8660aa5f5e0651059a8496e6
SSDEEP:	768:wxXFBWlBwBU0nTS1VCJlXcbkA+Lx6yPqPJ5QQmpgae3D5sRkMCX:SXTSwt21Vm1AMx6yPYJ5QQQgae3DsCX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L...kg.O.....0.....@.....

File Icon

Icon Hash:	b038b57269717938

Static PE Info

General

Entrypoint:	0x401394
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:	0x4F81676B [Sun Apr 8 10:24:43 2012 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:	f783b7553c2ee07b6bd756ebd3705f2c

Entrypoint Preview

Instruction
push 0040A6E0h
call 00007FA66089B4D5h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
loopne 00007FA66089B554h
mov al, 16h
add byte ptr [718C4333h], dl
dec edx
sbb dword ptr [edx+00FCBB1Ah], ecx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebp+esi*2+6Ch], dl
popad
jnc 00007FA66089B54Bh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or dl, dh
cmp al, C2h
jle 00007FA66089B50Fh
mov ah, 7Eh
inc ecx
mov ebx, dword ptr [eax+24088438h]
in al, dx
and al, A6h

Instruction
mov esp, 2BED4657h
dec eax
sbb byte ptr [ecx], 00000074h
std
in al, 88h
pop edi
popad
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push ebx
xchg eax, edx
add byte ptr [eax], al
push es
or al, 00h
add byte ptr [eax], al
pop es
add byte ptr [eax+6Fh], dl
jne 00007FA66089B555h
jnc 00007FA66089B54Bh
add byte ptr [67000701h], cl
jnc 00007FA66089B549h
jc 00007FA66089B555h
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx
add byte ptr [edx], ah
add byte ptr [ebx], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xee94	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xf76	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x11c	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xe388	0xf000	False	0.380240885417	data	5.87430872386	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1210	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xf76	0x1000	False	0.32861328125	data	3.68519752402	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x12c8e	0x2e8	data		
RT_ICON	0x123e6	0x8a8	data		
RT_GROUP_ICON	0x123c4	0x22	data		
RT_VERSION	0x12120	0x2a4	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaLenBstrB, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	OPDATERINGSDISKETTES
FileVersion	1.00
CompanyName	Wang
ProductName	Wang Laboratories
ProductVersion	1.00
FileDescription	Wang Laboratories
OriginalFilename	OPDATERINGSDISKETTES.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: OPDATERINGSDISKETTES.exe PID: 4316 Parent PID: 5636

General

Start time:	01:15:47
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\OPDATERINGSDISKETTES.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OPDATERINGSDISKETTES.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	446701E67DD00E1D2C45B23263533DEA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 1948 Parent PID: 4316

General

Start time:	01:17:03
Start date:	25/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\OPDATERINGSDISKETTES.exe'
Imagebase:	0x690000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5788 Parent PID: 1948

General

Start time:	01:17:04
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis