ID: 411100
Sample Name: Lista produkt#U00f3w.exe
Cookbook: default.jbs
Time: 16:11:34
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

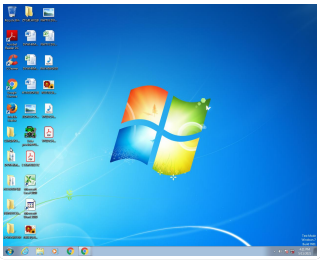
Analysis Report Lista produkt#U00f3w.exe

Overview

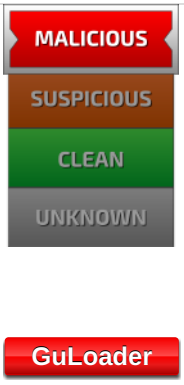
General Information

Sample Name:	Lista produkt#U00f3w.exe
Analysis ID:	411100
MD5:	c7f305d2e4f5e91..
SHA1:	c477a3d238b96c..
SHA256:	0d28b94959edb7..
Infos:	

Most interesting Screenshot:



Detection

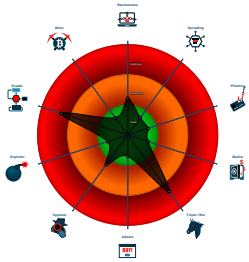


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Allocates memory within range whic…
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to query CPU …
- Contains functionality to read the PEB

Classification



Startup

- **System is w7x64**
- Lista produkt#U00f3w.exe (PID: 1492 cmdline: 'C:\Users\user\Desktop\Lista produkt#U00f3w.exe' MD5: C7F305D2E4F5E91E8118AC32EC796B0C)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=17FenSUBd1a7PqzhRX-elu4bxZvs0LF9Y"
}
```

Yara Overview

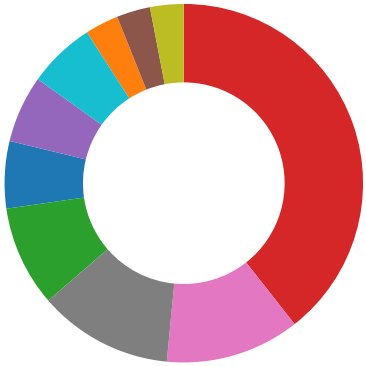
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.3167430661.0000000001D70000.00000040.00000001.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:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

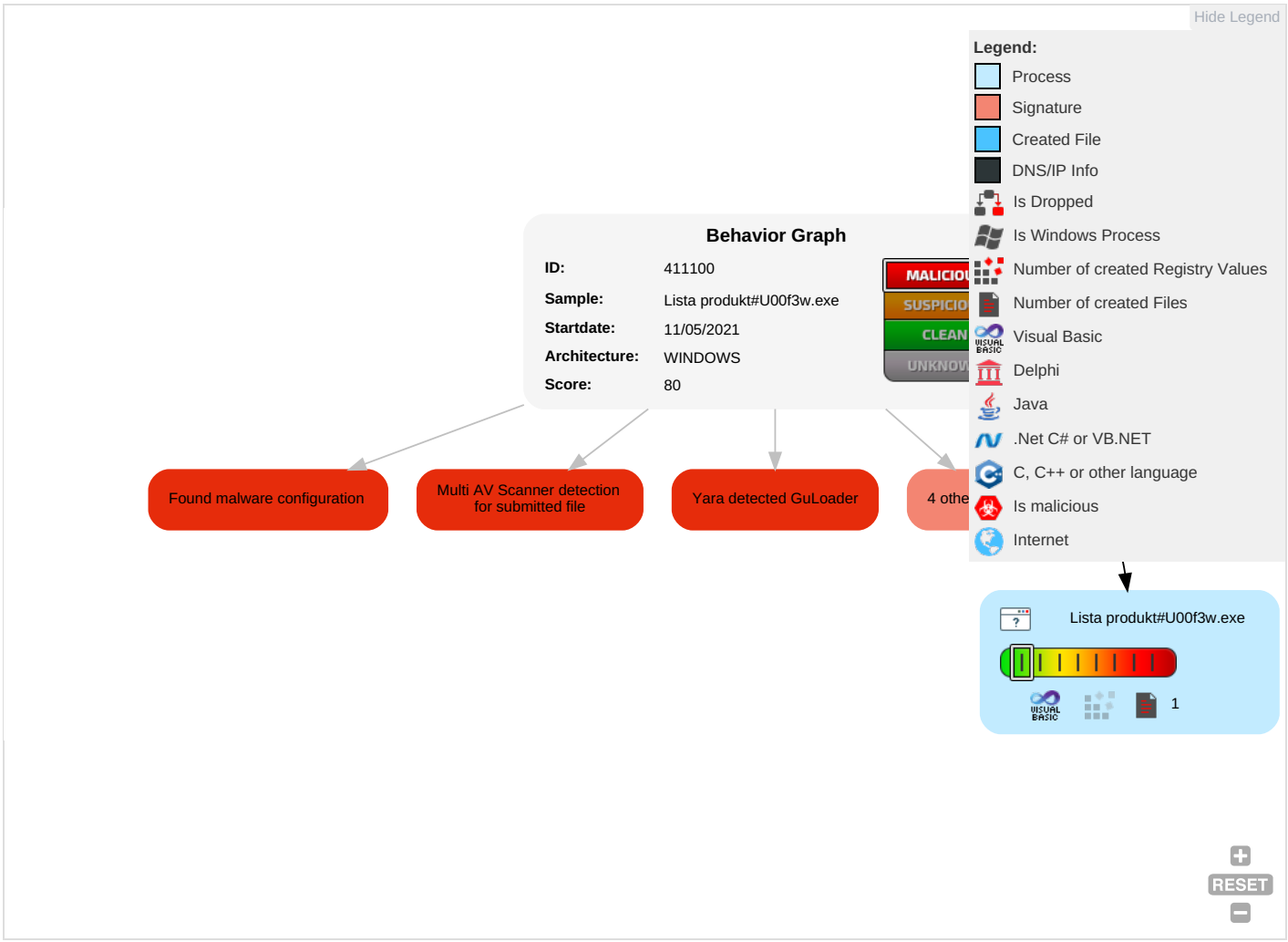
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
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	O D C B

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

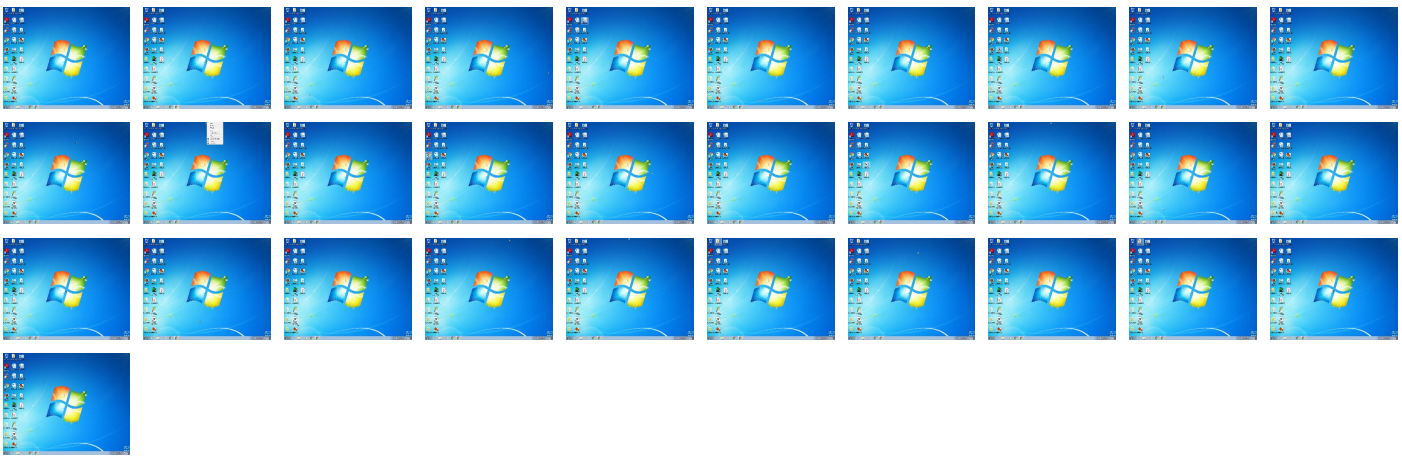
Behavior Graph



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
Lista produkt#U00f3w.exe	34%	Virustotal		Browse
Lista produkt#U00f3w.exe	17%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168905603.00000 00003647000.00000002.00000001. sdmp	false		high
http://www.windows.com/pctv.	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168785172.00000 00003460000.00000002.00000001. sdmp	false		high
http://investor.msn.com	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168785172.00000 00003460000.00000002.00000001. sdmp	false		high
http://www.msnbc.com/news/ticker.txt	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168785172.00000 00003460000.00000002.00000001. sdmp	false		high
http://www.icra.org/vocabulary/.	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168905603.00000 00003647000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168905603.00000 00003647000.00000002.00000001. sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168785172.00000 00003460000.00000002.00000001. sdmp	false		high
http://investor.msn.com/	Lista produkt#U00f3w.exe, 0000 0000.00000002.3168785172.00000 00003460000.00000002.00000001. sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411100
Start date:	11.05.2021
Start time:	16:11:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lista produkt#U00f3w.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.8% (good quality ratio 15.9%) • Quality average: 28.9% • Quality standard deviation: 34.1%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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):	5.711108381776406
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:	Lista produkt#U00f3w.exe
File size:	81920
MD5:	c7f305d2e4f5e91e8118ac32ec796b0c
SHA1:	c477a3d238b96c2a58e77bb7c818775e23f7d656
SHA256:	0d28b94959edb70309a2754a83f2c9230b3176618ab571995d81955751ca2dbe
SHA512:	6eebcaff0963b5a69f574ceb0eb11f07ac1e6a195476c32b863e026f825f563e6b2406f7e6f34cc2ade6515cb14980e2be471a010fc8c8cf8727faa4f1421b56
SSDEEP:	1536:cDMp+5asYexpjWzziwuVlCqRryDqRZkD:cV57+iwuV9RZk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....`.....0..... ....@.....

File Icon

Icon Hash:	b09298b8cc8a19c6

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:	0x6099DDA9 [Tue May 11 01:28:09 2021 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:	ec8e962978786706cf0189109090c85e

Entrypoint Preview

Instruction
push 00401F34h
call 00007F23AC9F8F63h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al

Instruction
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [edx+ecx*2-47h], cl
aas
mov byte ptr [ebx+0Bh], dh
inc edi
mov eax, 8AB5048Eh
les ecx, fword ptr [edx+09h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
call 00007F23F8A29D04h
push ebp
dec ebp
dec ecx
dec esi
dec ecx
inc esi
dec ecx
inc ebx
inc ebp
dec esi
push esp
add byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
push es
into
sbb bh, byte ptr [esi]
or esp, dword ptr [eax+56B54785h]
jnp 00007F23AC9F8FD3h
or eax, dword ptr [edi+33h]
push ebp
jc 00007F23AC9F8F35h
sub dword ptr [esi-6Eh], edx
xchg byte ptr [edi+eax*2], dh
xchg dword ptr [ebp-3B91C6C1h], edx
push ebp
pop eax
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

Instruction
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
cmp byte ptr [edx], cl
add byte ptr [eax], al
and al, 09h
add byte ptr [eax], al
add byte ptr [edi], al
add byte ptr [edx+65h], al
arpl word ptr [ebp+72h], si
jnc 00007F23AC9F8FD7h
add byte ptr [47001201h], cl
jc 00007F23AC9F8FE7h
jo 00007F23AC9F8FE2h
jnc 00007F23AC9F8FD4h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x111d4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0xc1c	.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	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x158	.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	0x107d4	0x11000	False	0.422291475184	data	6.18941304283	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x12000	0x11f4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x14000	0xc1c	0x1000	False	0.291015625	data	3.0223027499	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x14374	0x8a8	data		
RT_GROUP_ICON	0x14360	0x14	data		
RT_VERSION	0x140f0	0x270	data	Chinese	Taiwan

Imports

DLL	Import

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenVar, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaI2I4, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaVarCopy, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	Farveskrmene
FileVersion	1.00
CompanyName	Asso Filler
ProductName	Asso Filler
ProductVersion	1.00
FileDescription	Asso Filler
OriginalFilename	Farveskrmene.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Lista produkt#U00f3w.exe PID: 1492 Parent PID: 3000

General

Start time:	16:12:40
Start date:	11/05/2021
Path:	C:\Users\user\Desktop\Lista produkt#U00f3w.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Lista produkt#U00f3w.exe'
Imagebase:	0x400000
File size:	81920 bytes
MD5 hash:	C7F305D2E4F5E91E8118AC32EC796B0C

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.3167430661.0000000001D70000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis