ID: 679326
Sample Name: sipari#U015f listem05.08.2022.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:32:08
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

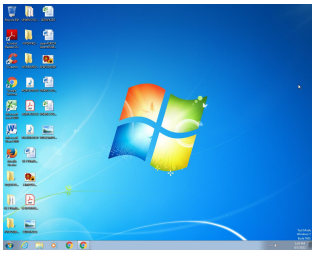
Windows Analysis Report

sipari#U015f listem05.08.2022.docx

Overview

General Information

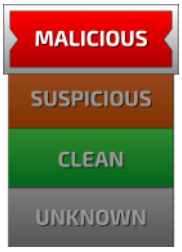
Sample Name:	sipari#U015f listem05.08.2022.docx
Analysis ID:	679326
MD5:	578f0e48afff4fa6..
SHA1:	112b4c96c4f74e...
SHA256:	c26c99eeb30da2..
Tags:	doc



Errors

⚠ Corrupt sample or wrongly selected analyzer.

Detection

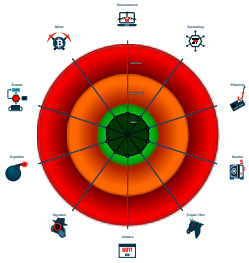


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Document contains OLE streams w…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2584 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

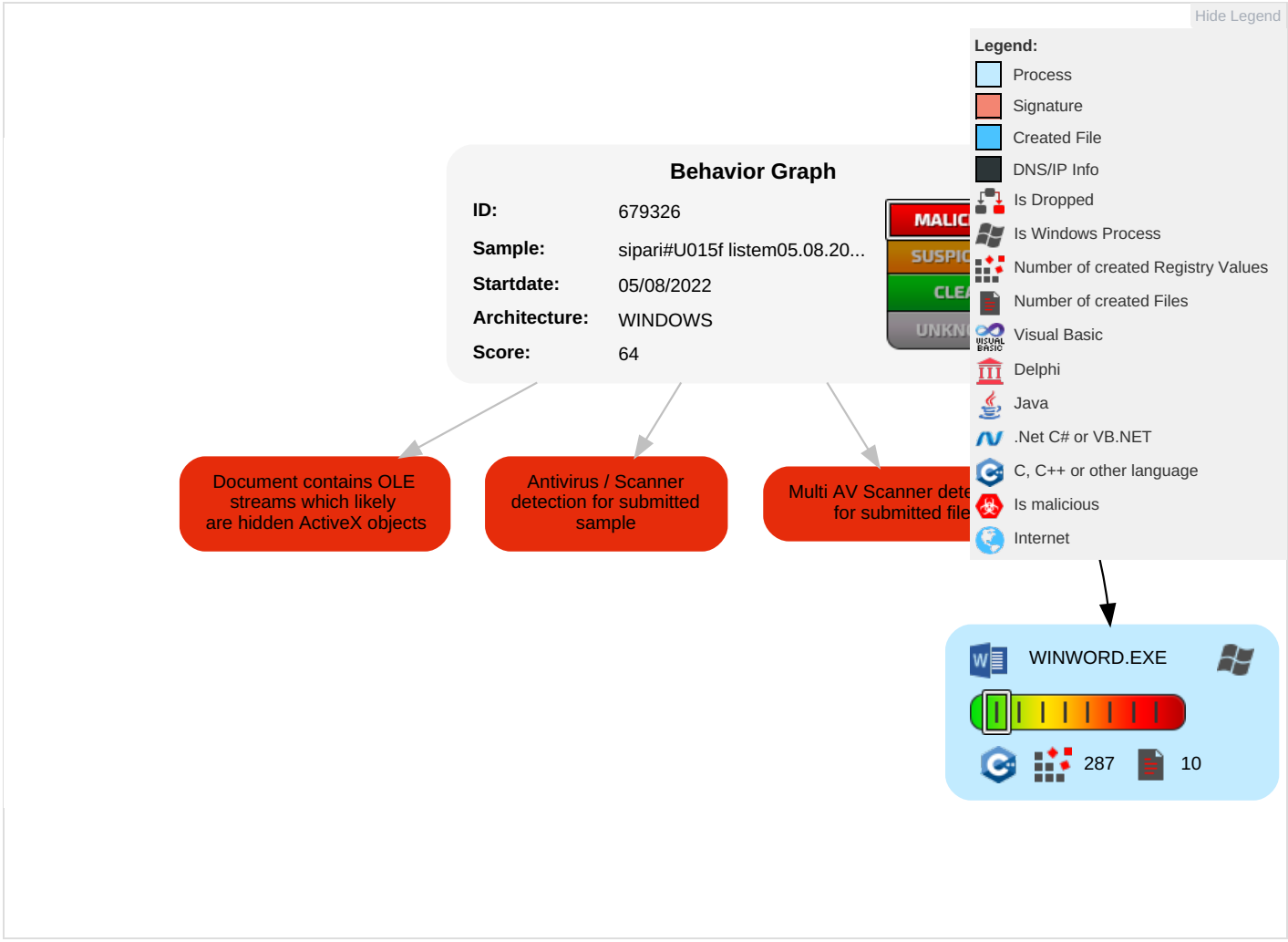
System Summary

Document contains OLE streams which likely are hidden ActiveX objects

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	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

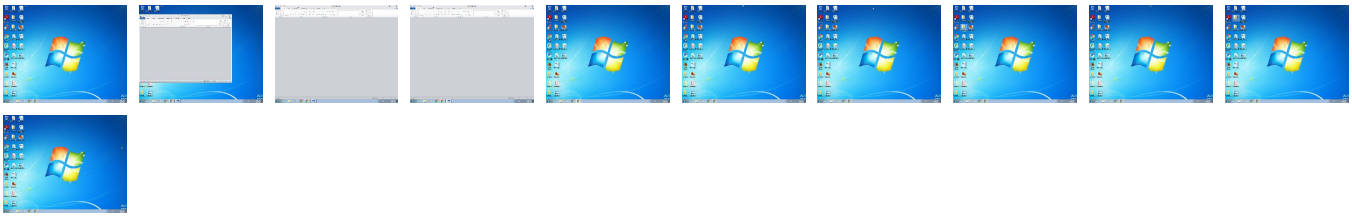
Behavior Graph



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
sipari#U015f listem05.08.2022.docx	11%	Virustotal		Browse
sipari#U015f listem05.08.2022.docx	100%	Avira	EXP/JAVA.Banload.VPDV.Gen	

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679326
Start date and time: 05/08/202215:32:08	2022-08-05 15:32:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	sipari#U015f listem05.08.2022.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	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:	mal64.winDOCX@1/3@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .docx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Errors

- Corrupt sample or wrongly selected analyzer.

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{59875063-1047-4CC6-A2F3-A0F4C03CF2F3}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525

Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\Desktop\~$pari#U015f listem05.08.2022.docx

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.981533951389543
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	sipari#U015f listem05.08.2022.docx
File size:	313830
MD5:	578f0e48afff4fa6927f146b2c6c1cf3
SHA1:	112b4c96c4f74e5ef7c89110e59a499068cfcad9
SHA256:	c26c99eeb30da221f74dd0951f4b8de0207e5801b64cd8d2a1abf1f906668096
SHA512:	eea66103dc92fb676d983b06e98fdde25c70d25e14e2618d533d0a1e1ea2989f7e97219a670a348bee4ac95c5e67443366c5212d9ceae8c8fc843cc1bed9ebaf
SSDEEP:	6144:ssqlRSPLKGm5u5acjKnkk/DiQ3kKibOopOaxCJ9cOlbo03:7+GLqqjKnkvQ3Jib94aIJ9cOS3
TLSH:	EE642263D0240BADF4666E3CC76C1522E35AD4B3A99193053A86BEFDD702FFA46C084D
File Content Preview:	PK.....!.....T.....[Content_Types].xml ... (.....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/679326/sample/sipari#U015f listem05.08.2022.docx"	
Indicators	
Has Summary Info:	
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary	
Author:	MICROSOFT
Template:	Normal.dotm
Last Saved By:	MICROSOFT
Revion Number:	1
Total Edit Time:	1
Create Time:	2022-08-05T07:47:00Z
Last Saved Time:	2022-08-05T07:48:00Z
Number of Pages:	1
Number of Words:	3
Number of Characters:	21
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	14.0000

Streams	
Stream Path: \x1CompObj, File Type: data, Stream Size: 72	
General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	72
Entropy:	3.8231129765226823
Base64 Encoded:	False
Data ASCII:	. . . . / . { . . . Z @ . . . . P a c k a g e . . . . P a c k a g e . 9 q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 a7 0d f2 2f c0 ce 11 92 7b 08 00 09 5a e3 40 08 00 00 00 50 61 63 6b 61 67 65 00 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole, File Type: data, Stream Size: 20	
General	
Stream Path:	\x1Ole
File Type:	data
Stream Size:	20
Entropy:	0.8475846798245739
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 00 00 02 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x1Ole10Native, File Type: data, Stream Size: 173953

General	
Stream Path:	\x1Ole10Native
File Type:	data
Stream Size:	173953
Entropy:	7.995515846329769
Base64 Encoded:	True
Data ASCII:	} . . . . L W I U Y V B D K U V B F D R I S C A U K O O O Q J F J F E M O P L Y G C T L M W K N T J Q K D . J A R . C : \\ U s e r s \\ M I C R O S O F T \\ A p p D a t a \\ L o c a l \\ M i c r o s o f t \\ W i n d o w s \\ I N e t C a c h e \\ C o n t e n t . W o r d \\ L W I U Y V B D K U V B F D R I S C A U K O O O Q J F J F E M O P L Y G C T L M W K N T J Q K D . J A R . . . . . C : \\ U s e r s \\ M I C R O S ~ 1 \\ A p p D a t a \\ L o c a l \\ T e m p \\ { E F 6 6 F A 5 B - F 6 8 5 - 4 C 2 B - 8 C 3 2 - A 9
Data Raw:	7d a7 02 00 02 00 4c 57 49 55 59 56 42 44 4b 55 56 42 46 44 52 49 53 43 41 55 4b 4f 4f 4f 51 4a 46 4a 46 45 4d 4f 50 4c 59 47 43 54 4c 4d 57 4b 4e 54 4a 51 4b 44 2e 4a 41 52 00 43 3a 5c 55 73 65 72 73 5c 4d 49 43 52 4f 53 4f 46 54 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 43 6f 6e 74 65 6e 74 2e

Stream Path: \x3ObjInfo, File Type: data, Stream Size: 6	
General	
Stream Path:	\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.7924812503605778
Base64 Encoded:	False
Data ASCII:	@ . . . . .
Data Raw:	40 00 03 00 01 00

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: **2584**, Parent PID: **576**

General	
Target ID:	0
Start time:	15:33:14
Start date:	05/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13faa0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly