

JoeSandbox Cloud BASIC



ID: 682568

Sample Name: wpswireless-
invoice-08.11.22.doc

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 17:40:50

Date: 11/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report wpswireless-invoice-08.11.22.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	5
AV Detection	5
Software Vulnerabilities	5
System Summary	5
Mitre Att&ck Matrix	5
Behavior Graph	5
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
World Map of Contacted IPs	9
Public IPs	9
General Information	9
Warnings	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	11
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rm[1].htm	11
C:\Users\user\AppData\Local\Temp\6A2E.tmp.dll	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\wpswireless-invoice-08.11.22.LNK	11
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	12
C:\Users\user\Desktop\~\$wireless-invoice-08.11.22.doc	12
Static File Info	12
General	12
File Icon	13
Static OLE Info	13
General	13
OLE File "opt/package/joesandbox/database/analysis/682568/sample/wpswireless-invoice-08.11.22.doc"	13
Indicators	13
Streams with VBA	13
VBA File Name: ThisDocument.cls, Stream Size: 2739	13
General	13
VBA Code	13
Streams	13
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	13
General	13
Stream Path: PROJECTwm, File Type: data, Stream Size: 41	14
General	14
Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	14
General	14
Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5100	14
General	14
Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724	14
General	14
Stream Path: VBA/dir, File Type: data, Stream Size: 486	14
General	14
Network Behavior	15
TCP Packets	15
HTTP Request Dependency Graph	15
HTTP Packets	15
Statistics	16
System Behavior	16
Analysis Process: WINWORD.EXEPID: 1448, Parent PID: 576	16

General	16
File Activities	16
File Created	16
File Deleted	17
File Written	17
File Read	18
Registry Activities	18
Key Created	18
Disassembly	18

Windows Analysis Report

wpswireless-invoice-08.11.22.doc

Overview

General Information

Sample Name:

wpswireless-invoice-08.11.22.doc

Analysis ID:

682568

MD5:

672ff75cfa22373..

SHA1:

02dd6b448c2373..

SHA256:

aabc9295e27a67..

Tags:

doc

icedID

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Document exploit detected (creates...

Multi AV Scanner detection for subm...

Document contains an embedded V...

Document exploit detected (UrlDown...

Machine Learning detection for sam...

Potential document exploit detected ...

Uses a known web browser user age...

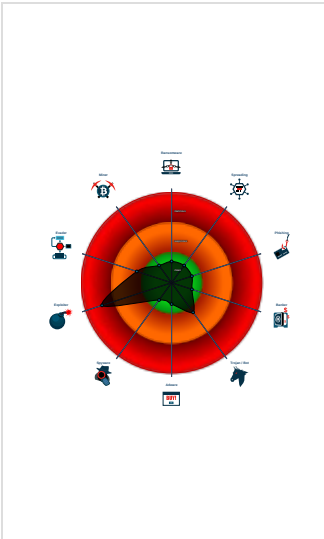
Document contains an embedded V...

Document contains embedded VBA...

Potential document exploit detected...

IP address seen in connection with ...

Classification



Process Tree

- System is w7x64
- WINWORD.EXE (PID: 1448 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



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities



Document exploit detected (creates forbidden files)

Document exploit detected (UrlDownloadToFile)

System Summary

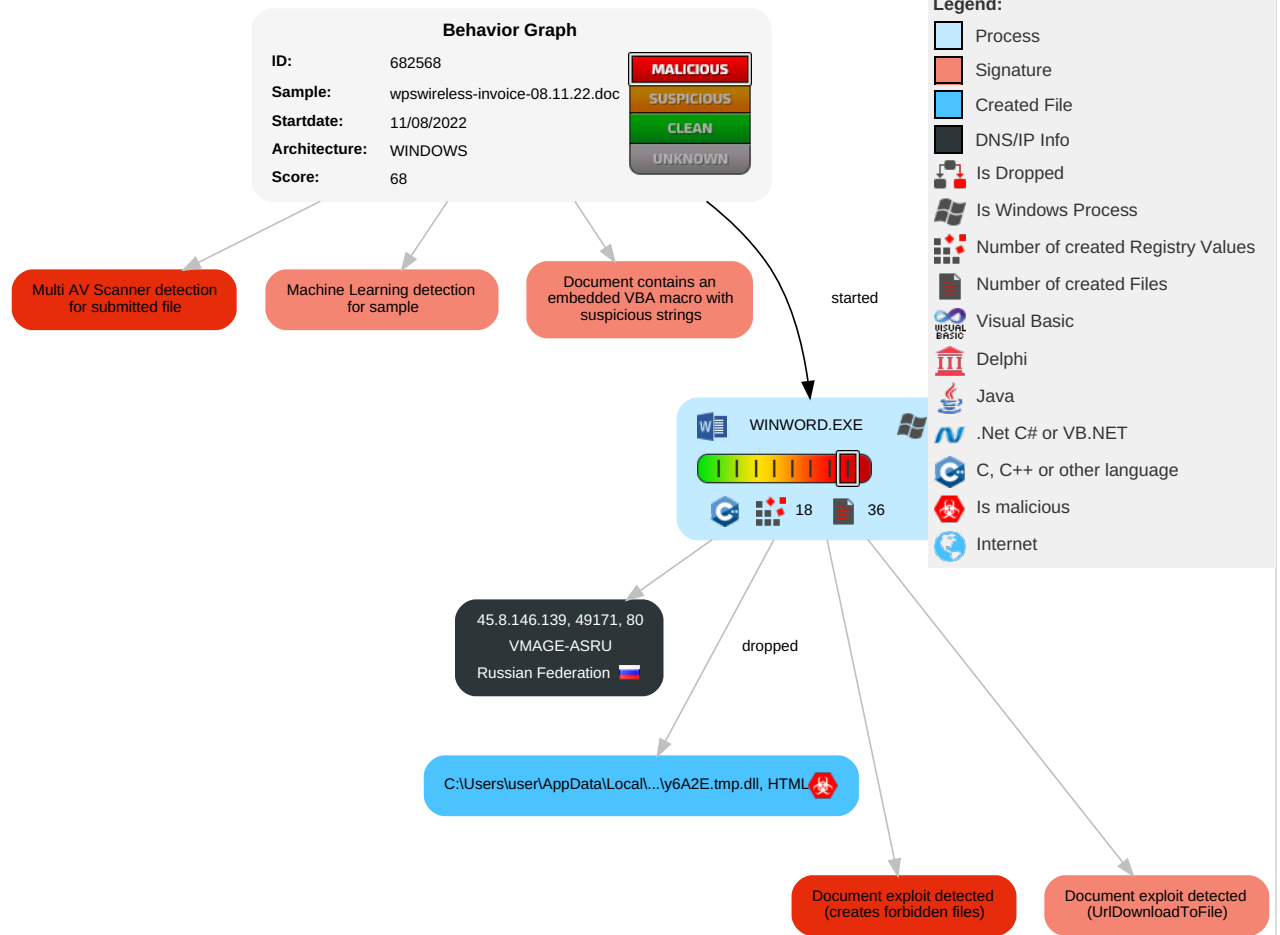


Document contains an embedded VBA macro with suspicious strings

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	1 2 Scripting	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 Non-Application Layer Protocol	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 2 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 2 Scripting	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

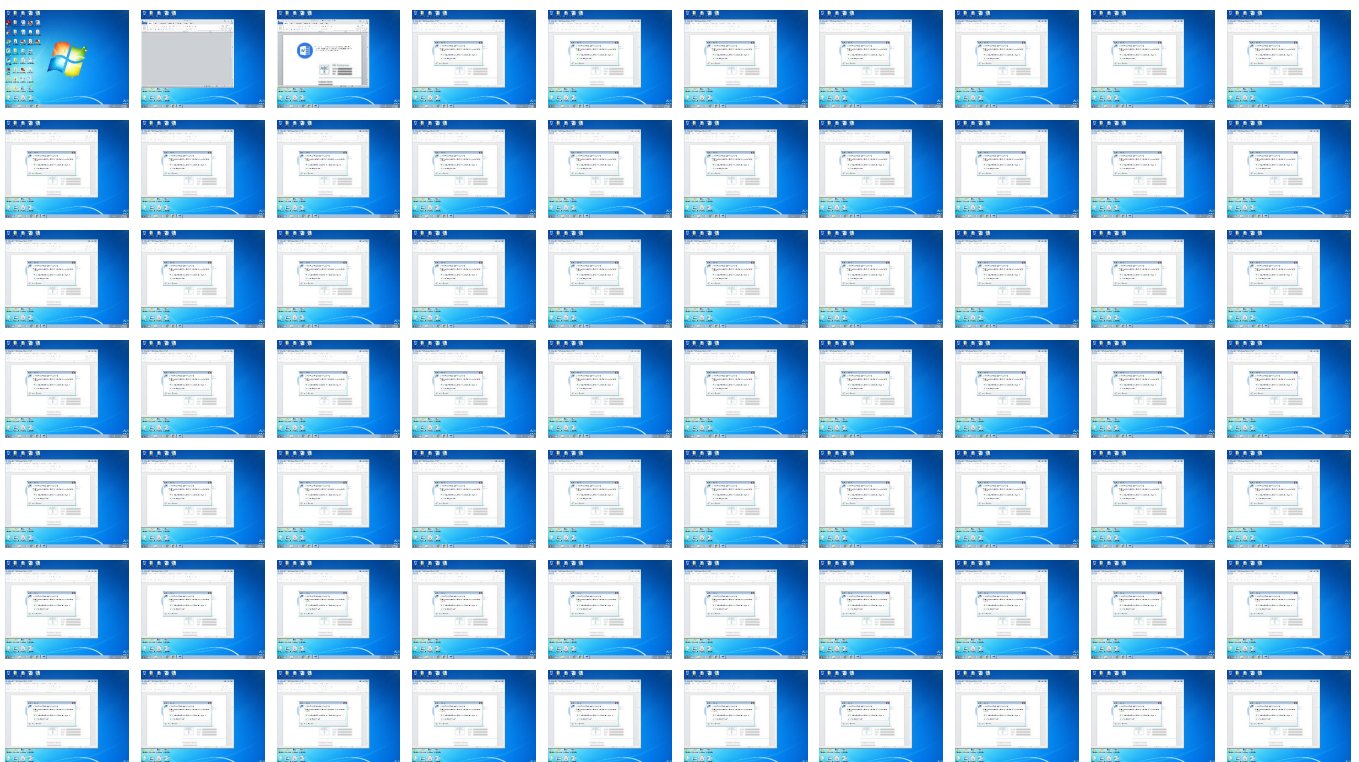
Behavior Graph

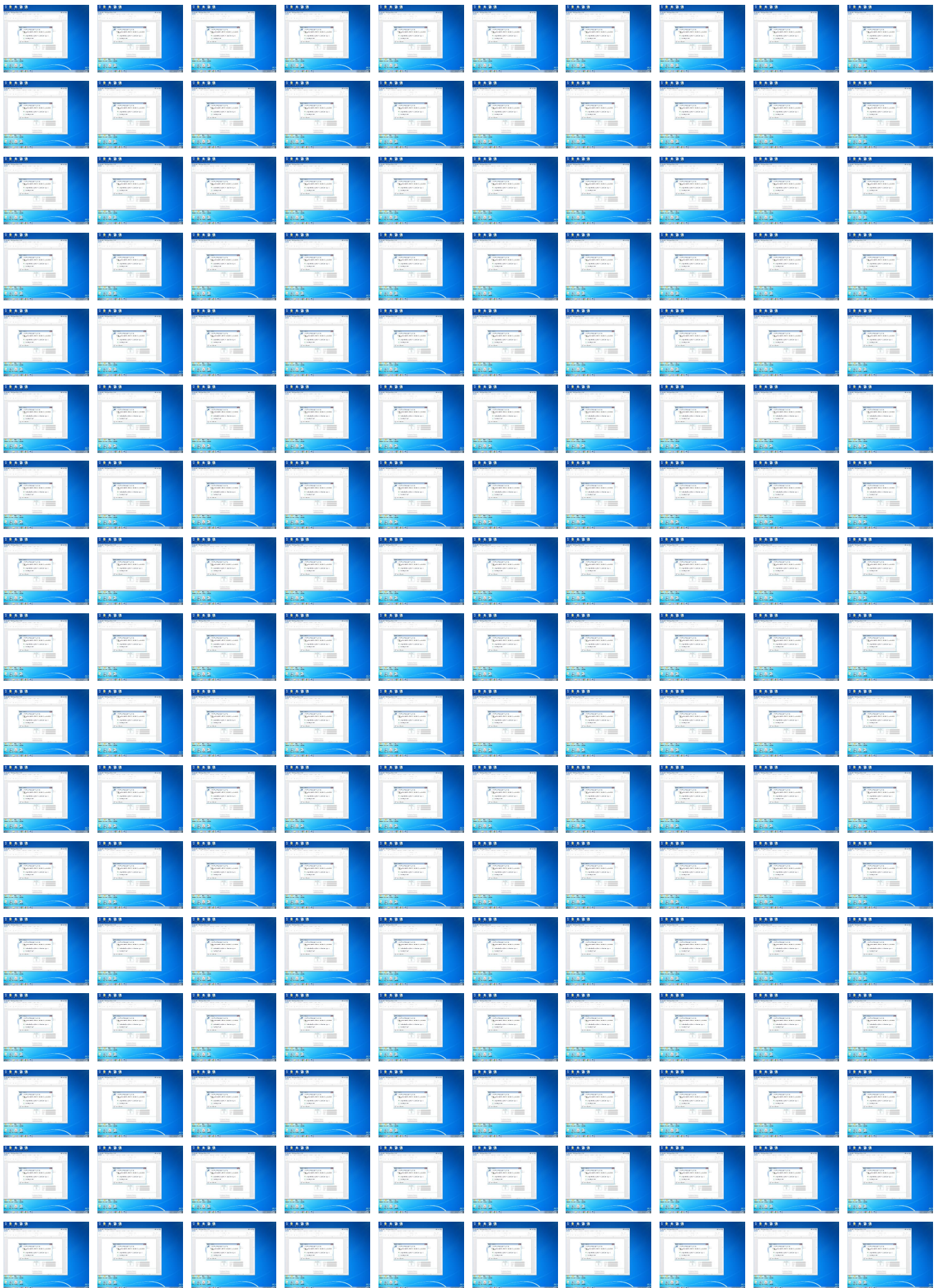


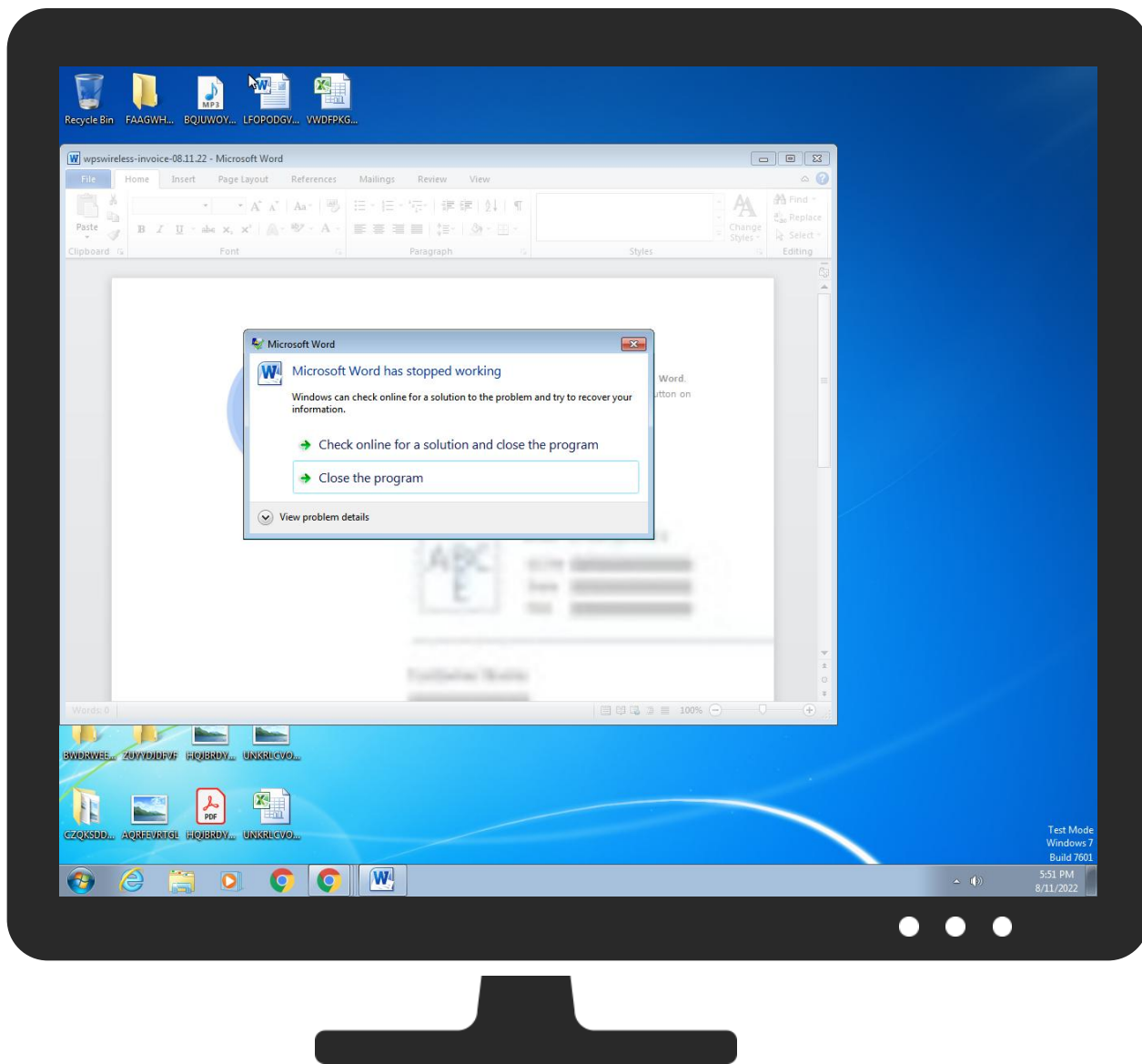
Screenshots

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
wpswireless-invoice-08.11.22.doc	22%	Virustotal		Browse
wpswireless-invoice-08.11.22.doc	15%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
wpswireless-invoice-08.11.22.doc	100%	Joe Sandbox ML		

Dropped Files

🚫 No Antivirus matches

Unpacked PE Files

🚫 No Antivirus matches

Domains

🚫 No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.8.146.139/fhfty/_C45V3_-S5YKINT86D3PPVX0ILQLA-SG/rm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

🚫 No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/_C45V3_-S5YKINT86D3PPVX0ILQLA-SG/rm	false	Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682568
Start date and time:	2022-08-11 17:40:50 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wpswireless-invoice-08.11.22.doc
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:	6
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winDOC@1/6@0/1
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: .doc • Adjust boot time • Enable AMSI

Warnings

- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.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.IE5\ZAE7RW1P\rm[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.110875983732391
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGOBRmEr6VnetdzRx3bIGKCezocKqD:J0+oxBeRmR9etdzRxbIYez1T
MD5:	6DFF44B8B60DD046290A5420717F052E
SHA1:	2339B6BC052682B5CC618733AEEE776037485D3E
SHA-256:	2E519B2E823E2503B635A59BBC29A00170F18F86BC7F5330563188B105FF87D7
SHA-512:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C4880763
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "rm" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\y6A2E.tmp.dll 

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	modified
Size (bytes):	201
Entropy (8bit):	5.110875983732391
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGOBRmEr6VnetdzRx3bIGKCezocKqD:J0+oxBeRmR9etdzRxbIYez1T
MD5:	6DFF44B8B60DD046290A5420717F052E
SHA1:	2339B6BC052682B5CC618733AEEE776037485D3E
SHA-256:	2E519B2E823E2503B635A59BBC29A00170F18F86BC7F5330563188B105FF87D7
SHA-512:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C4880763
Malicious:	true
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "rm" was not found on this server. .</body></html>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	107
Entropy (8bit):	4.724609804997727
Encrypted:	false
SSDEEP:	3:bDuMJIKCsAWWIKGHjXbUmX1mWfsAWWIKGHjXbUv:bC0s+GHjXbSgs+GHjXb2
MD5:	6D22B1B60083716F1E8936205BB774BE
SHA1:	E0BF33F423B44E56CE3507E5D0F6E4A62D6F46B6
SHA-256:	A2F799C1F3ECF0CC33F6001EEB53D6DECFO31021A4749D88506141300BAA0710
SHA-512:	D6BBBA16D4A4D27183D85129F9781D9D67E9A3DB3A2984639079451B802FCAA5F39DE2BEF15AA1BC811C9D537FCC82166DAB165AB8DC392142365E2FD2EF8C7B
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..wpswireless-invoice-08.11.22.LNK=0..[doc]..wpswireless-invoice-08.11.22.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\wpswireless-invoice-08.11.22.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Thu Aug 11 23:42:11 2022, length=2256213, window=hide

Category:	dropped
Size (bytes):	1104
Entropy (8bit):	4.5553022924144395
Encrypted:	false
SSDEEP:	12:8Qe/E5gXg/XAICPCHaXRBkBt/eLX+Wixcf/xgimWelrzcivbLKG+vJxjBlrzXDz:8L0/XThOMT/xfhuevL+vrYXDv3q5u7D
MD5:	B4B7FA7B14E57592EFA69AD120088456
SHA1:	27E08344D8FFFF2FDA63799F345626B3D65B82C9
SHA-256:	A9ED81374781763EE477182C7626BCBAC7EDA73979666CAB090FAF8AF4CD14B8
SHA-512:	43832A323B8AB8ECDAE4E015E3EA68C32A8075A47C2A502E1FC3BCECDFE3E1905E05EBFB07F16ED04B975187028B961410A5A9524A872CEDC9CEC0C5FE5D3205
Malicious:	false
Reputation:	low
Preview:	L.....F.....\$...3...\$...3...[...Um".....P.O. :i.....+00.../C:\.....t1.....QK.X..Users.`.....:QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....L.1.....hT.....user.8.....QK.XhT.*...&=...U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT.*..._...=.....:D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.Um".UF. .WPSWIR~1.DOC..n.....hT..hT.*...r.....'.....w.p.s.w.i.r.e.l.e.s.s.-.i.n.v.o.i.c.e.-.0.8...1.1...2.2...d.o.c.....-...8...[.....?J.....C:\U sers\.#.....\445817\Users.user\Desktop\wpswireless-invoice-08.11.22.doc.7.....\.....\.....\.....\D.e.s.k.t.o.p.\w.p.s.w.i.r.e.l.e.s.s.-.i.n.v.o.i.c.e.-.0.8...1.1...2.2...d.o.c.....:,LB.)...Ag.....1SPS.XF.L8C....&m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....

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:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/In:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AFA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\Desktop\~\$swireless-invoice-08.11.22.doc	
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:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/In:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AFA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info	
General	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.994091181083785

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:	wpswireless-invoice-08.11.22.doc
File size:	2350727
MD5:	672ff75cfa223733b4d42382089a57b2
SHA1:	02dd6b448c2373dc1223724b1ab1aff920528aa6
SHA256:	aabc9295e27a673dcfb902960b8196a561923cef78ddb061956cb627fcfa782c
SHA512:	67ae70869362e5f55cec2655cbe924387baed91a0104abfb47ead979aac7b56684af5e5413b305ea1fdaeb5ccd7053e7ff398a341dd2fcc7c8b325f05ac2e272
SSDEEP:	49152:eT3UFkBP a/06xtvpz126ejPDkZ3T4EtUxFc2mpXfQK9B:qUke3v912tAJT45xF6pXfQK7
TLSH:	3BB533A9751FE67ED0C8DE700D12EA9433A7E9DE4AC8049CC234CAD21DFC225B55F85A
File Content Preview:	PK.....!..U~....._rels/.rels...J.@.....4.E..D.....\$....T..w-.j..... .zs..z..z.*X.%(v.....6O.{PI.....`S__x.C..CR.....t.R.....hl.3..H.Q..*.;..=..y... n.....yo.....[vrf..A..6..3]>_...-K.....\NH!....<..r...E.B..P...<_.

File Icon	
	
Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info	
General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682568/sample/wpswireless-invoice-08.11.22.doc"	
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:	True

Streams with VBA	
VBA File Name: ThisDocument.cls, Stream Size: 2739	
General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2739
Data ASCII:	...Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.Spac.IFa.Ise.JCrea.tabl..Pre decla..Id..#Tru."Expose..Temp.lateDeriv.\$CustomlizC.P.....D.? PtrSa.fe FunctionLib "user.32" Alias "SetTimer" (ByVal As Longy.1,
Data Raw:	01 0e b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

VBA Code	

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators

General	
Stream Size:	365
Entropy:	5.260544526473288
Base64 Encoded:	True
Data ASCII:	ID="{C6A0317C-67D6-49C1-8B70-93806A50A3CE}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="EBE92259095D095D095D095D"..DPB="D6D41F76E18ACD8BCD8BCD"..GC="C1C3088D098D0972"....[Host Extend er Info]..
Data Raw:	49 44 3d 2d 7b 43 36 41 30 33 31 37 43 2d 36 37 44 36 2d 34 39 43 31 2d 38 42 37 30 2d 39 33 38 30 36 41 35 30 41 33 43 45 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, **File Type:** ISO-8859 text, with no line terminators, **Stream Size:** 7

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00

Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5100

[illegible]

Stream Path: VBA/___SRP_3, **File Type:** data, **Stream Size:** 2724

[illegible]

Stream Path: VBA/dir, File Type: data, Stream Size: 486

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486

General	
Entropy:	6.296812220423808
Base64 Encoded:	True
Data ASCII:	0.....H.....Project.Q(..@.....=...l.....Ad-...".<...rstdo.le>..s.t..d.o.l.e.(..h..^.*\\..G{00020430-....C.....46}#2.0#.0#C:\\Win.dows\\sys@tem32\\e2..tlb#OLE. Automati.on.ENor (maIENCr.m.aF... cEC.....m.! OfficgO.f.i.cg..g2DF8D0.4C-5BFA
Data Raw:	01 e2 b1 80 01 00 04 00 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 00 08 06 12 09 02 12 80 07 41 f4 64 2d 00 0c 02 22 0a 3c 02 0a 16 02 72 73 74 64 6f 08 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 00 28 0d 00 68 00 11 5e 00 03 2a 5c 00 47 7b 30 30 30

Network Behavior

TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 17:41:43.854727030 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:41:43.958189011 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:41:43.958283901 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:41:43.958575010 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:41:44.061737061 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:41:44.084824085 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:41:44.084945917 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 17:41:49.090315104 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 17:41:49.090611935 CEST	49171	80	192.168.2.22	45.8.146.139

HTTP Request Dependency Graph	
45.8.146.139	

HTTP Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	45.8.146.139	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 17:41:43.958575010 CEST	0	OUT	GET /fhfty/_C45V3_-S5YKINT86D3PPVX0ILQLA-SG/rm HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 45.8.146.139 Connection: Keep-Alive
Aug 11, 2022 17:41:44.084824085 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 15:41:44 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 201 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "rm" was not found on this server. </body></html>

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1448, Parent PID: 576

General

Target ID:	0
Start time:	17:42:12
Start date:	11/08/2022
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:	0x13fdb0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6E1A2B14	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\6A2E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	75D54E7	GetTempFileNameA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	75D7C2D	URLDownloadToFileA
C:\Users\user\AppData\Local\Temp\6A2E.tmp.dll	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	75D7C2D	URLDownloadToFileA

File Deleted							
File Path				Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\6A2E.tmp				success or wait	1	75D555D	DeleteFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\rm[1].htm	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "rm" was not found on this server. </body></html>	success or wait	1	75D7C2D	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Temp6A2E.tmp.dll	0	201	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 72 6d 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html> <head><title>404 Not Found</title></head> <body> Not Found The requested URL "rm" was not found on this server. </body></html>	success or wait	1	75D7C2D	URLDownloadTo FileA

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E51A0EB	ReadFile	
C:\Users\user\AppData\Local\Temp\Temp6A2E.tmp.dll	unknown	4096	success or wait	1	7668805	ReadFile	
C:\Users\user\AppData\Local\Temp\Temp6A2E.tmp.dll	unknown	4096	end of file	1	7668805	ReadFile	

Registry Activities				
Key Created				
Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E1FA5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E1FA5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E1FA5E3	RegCreateKeyEx A

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								