ID: 682606
Sample Name:
valliant.document.08.11.2022.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:44:10
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

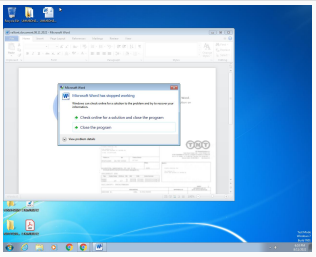
Windows Analysis Report

valliant.document.08.11.2022.doc

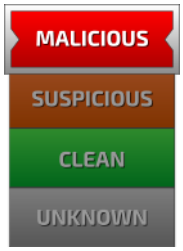
Overview

General Information

Sample Name:	valliant.document.08.11.2022.doc
Analysis ID:	682606
MD5:	cadb9d5ed47b8d..
SHA1:	f7197fa991510f9..
SHA256:	9cb01729327bd9..
Tags:	doc IcedID
Infos:	



Detection

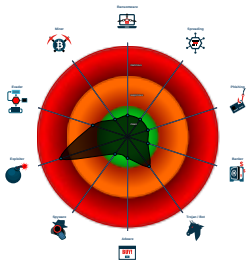


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates…
- Multi AV Scanner detection for subm…
- Document contains an embedded V…
- 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: 1540 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)

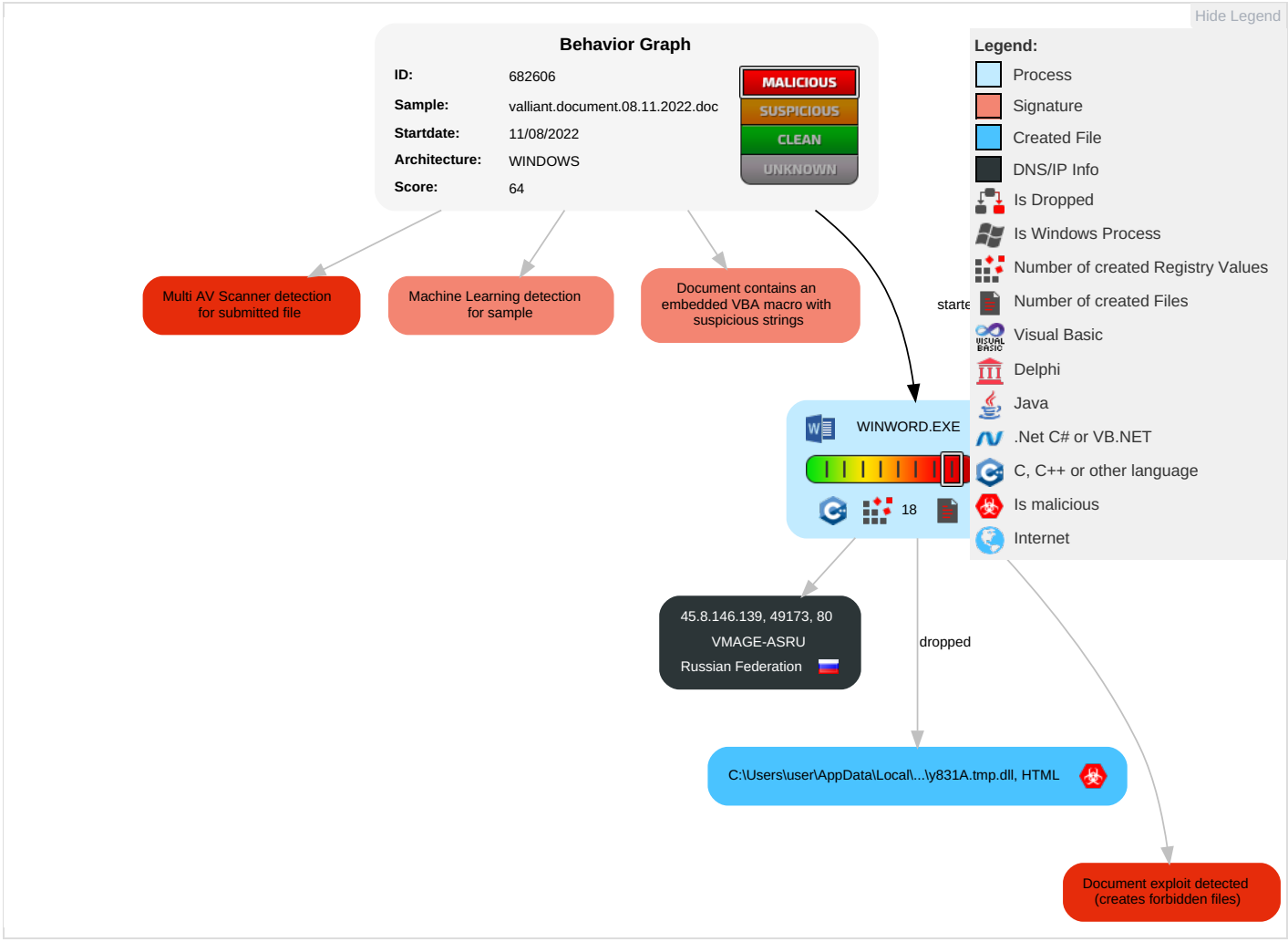
System Summary

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	1 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

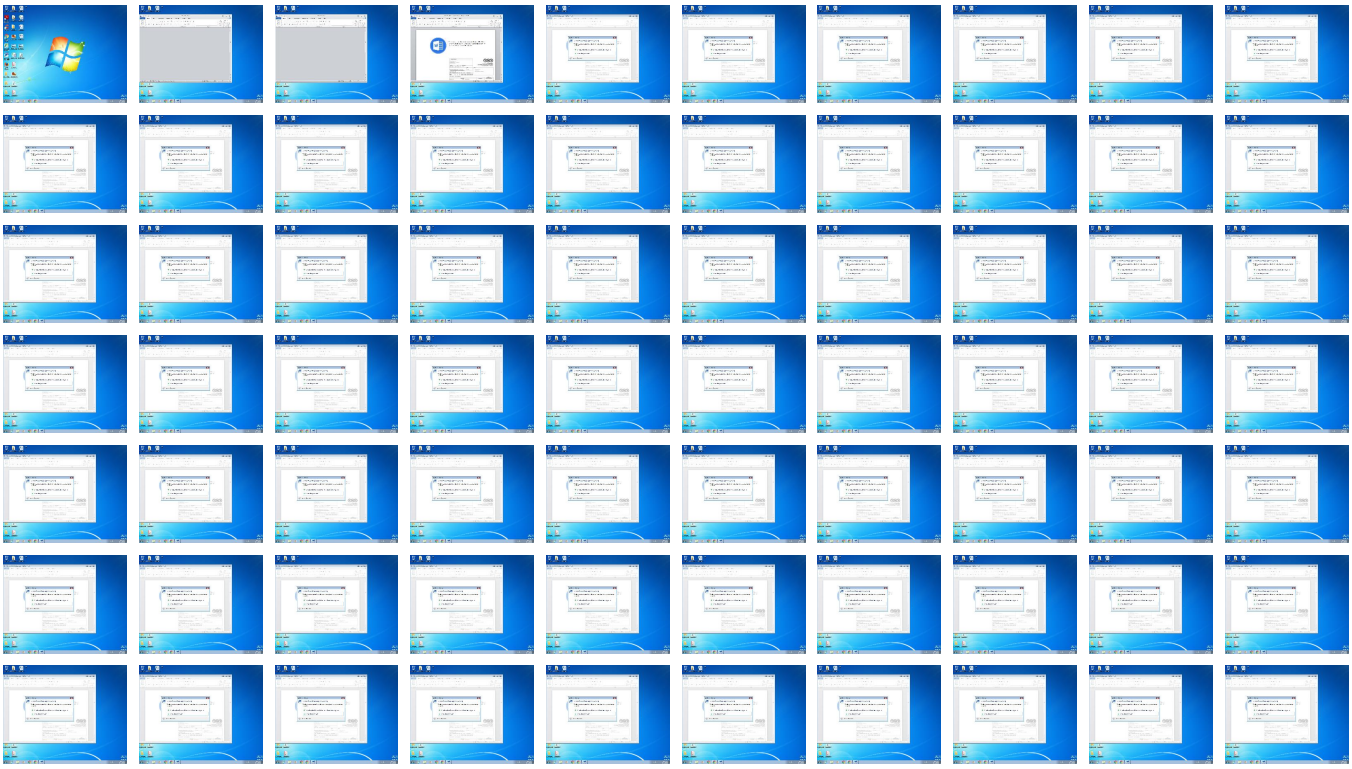
Behavior Graph

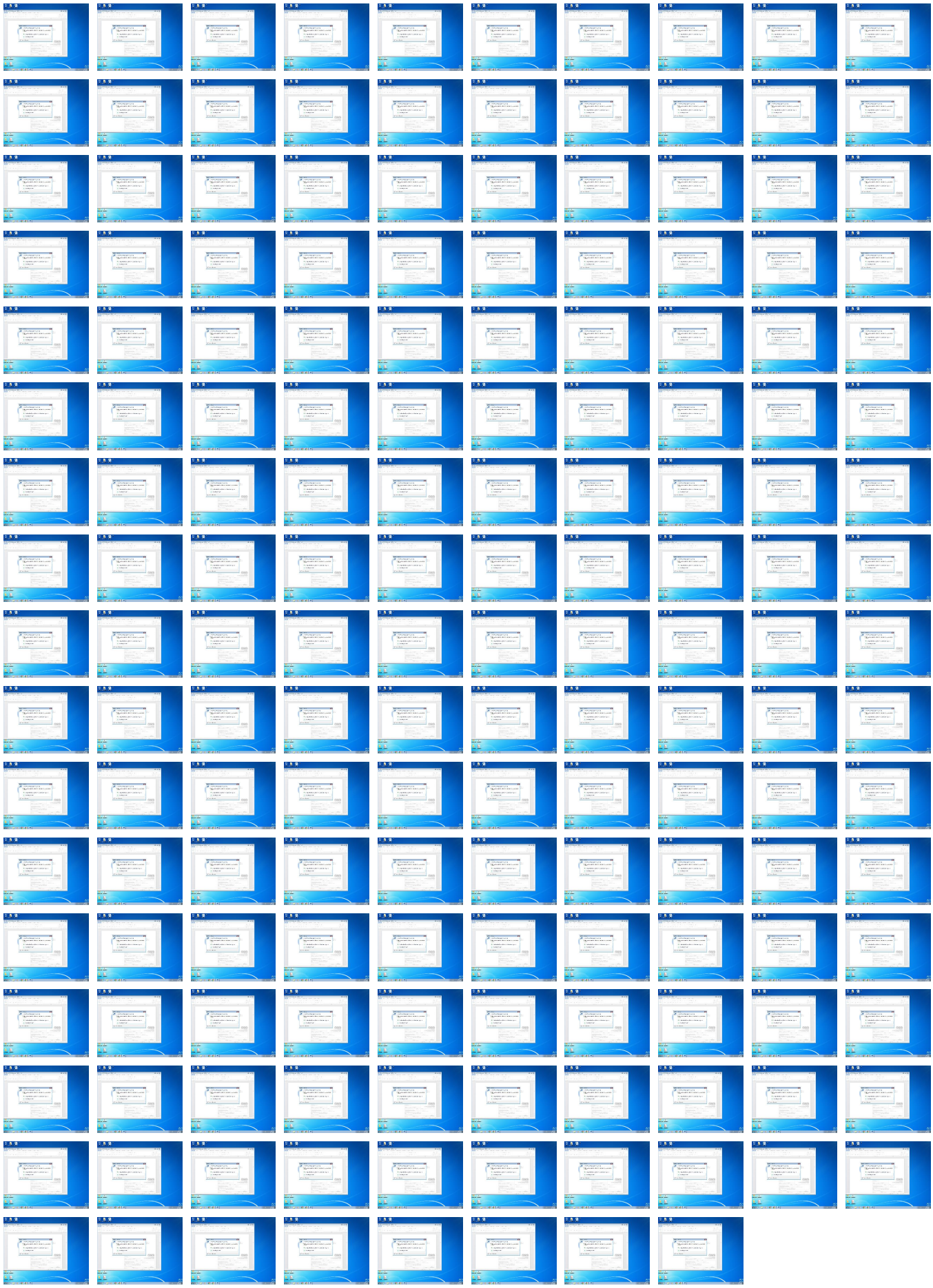


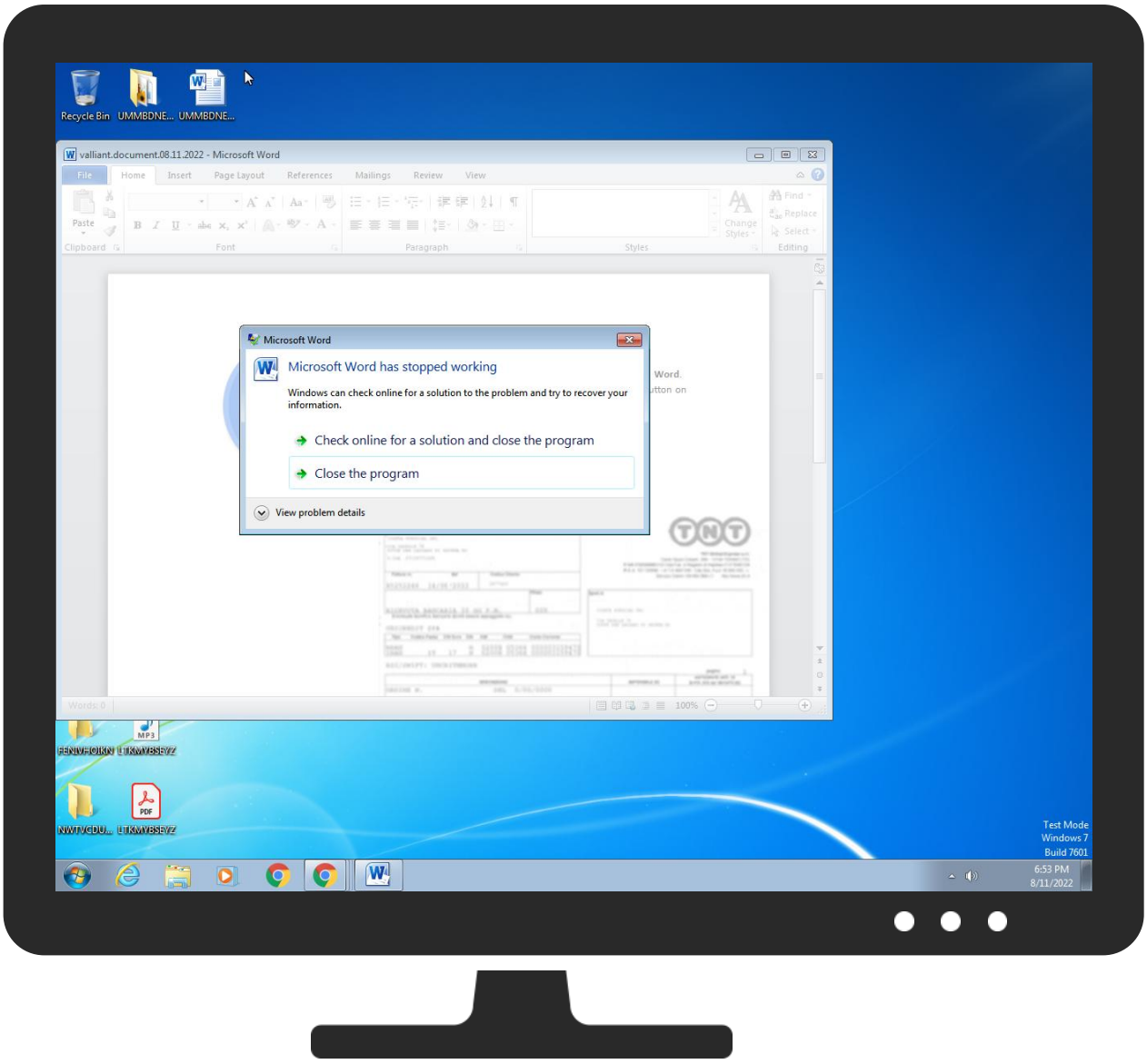
Screenshots

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
valliant.document.08.11.2022.doc	27%	Virustotal		Browse
valliant.document.08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
valliant.document.08.11.2022.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/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	0%	Avira URL Cloud	safe	

Domains and IPs

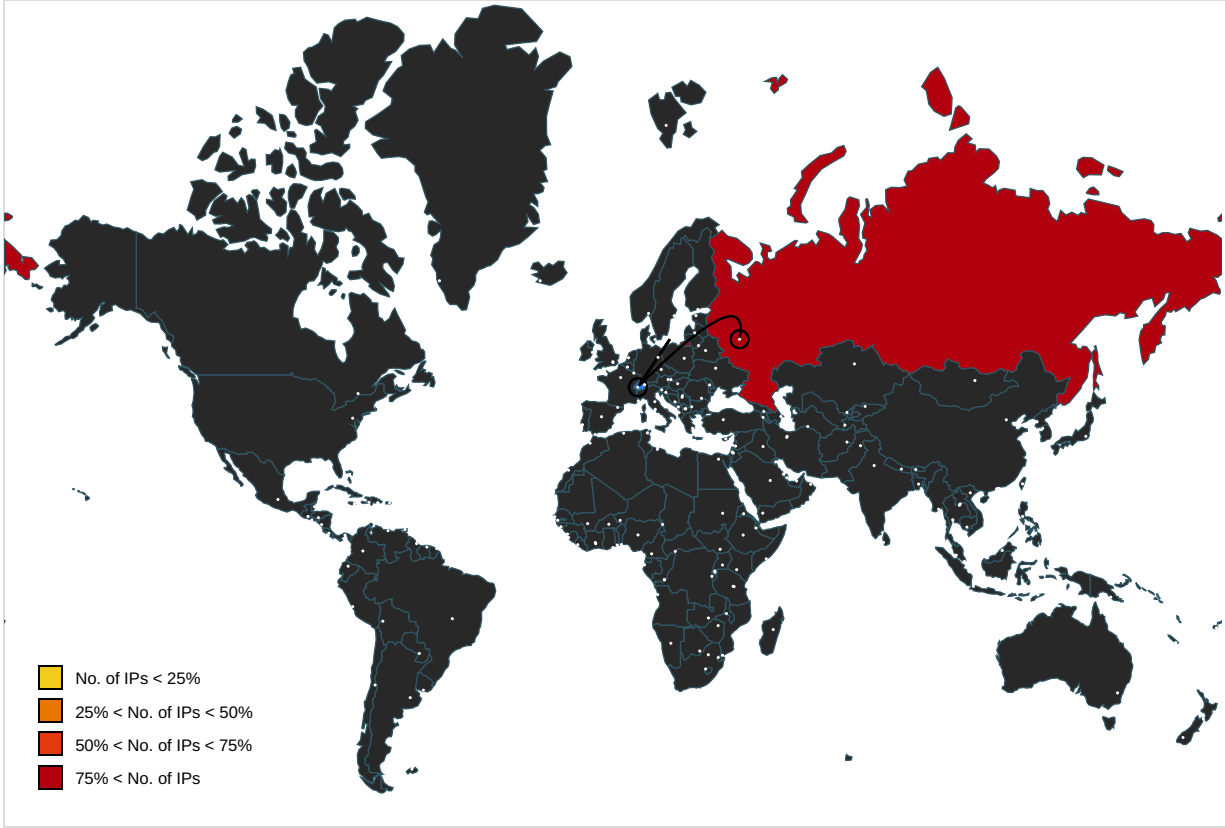
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f	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:	682606
Start date and time:	2022-08-11 18:44:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	valliant.document.08.11.2022.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:	mal64.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\-f[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	201
Entropy (8bit):	5.120826232488609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
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 "-f" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\y831A.tmp.dll

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	modified
Size (bytes):	201
Entropy (8bit):	5.120826232488609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3LZKCezocKqD:J0+oxBeRmR9etdzRxLFez1T
MD5:	33A7649A487B43D650E4D478C96E4588
SHA1:	F10EA1CC461B73EEE86CBE992CC4724F7B4C5175
SHA-256:	469501F44D054081AD49D1D0AB0B8031ECCE6986D17D346CC39DFB7BCF327F76
SHA-512:	24CDCCA259970B669949BD197AA55FD6E05D91B53A05984D3EBB3B219B6D26BDD67165967F1C8960D55E517D7AC46E1E515DD6E5C45DE4923F2FB1B1A98BCI 22
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 "-f" 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):	4.673221101791497
Encrypted:	false
SSDEEP:	3:bDuMJlLWRBKHIALRlj9omX10JFRBKHIALRlj9ov:bCAeB7ALr9lbB7ALr9y
MD5:	2135B655295683DA0D22CC6878E83DDE
SHA1:	EA560ECC587FEA774ACEA061F176B6A5698001CF
SHA-256:	3780877B180EE7F306F8141657DA6AD4F3C93B3866521397CC4F36A5472E94DC
SHA-512:	7C680FB5839D5025F6D5DA2AFF60D7293666F72CC8C8ADB2999FE72D2897A8C8C780EBCF8AAC6C8C18838589F5D2E407C858C826D45B3CA412044880F53AFF. E
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..valliant.document.08.11.2022.LNK=0..[doc]..valliant.document.08.11.2022.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\valliant.document.08.11.2022.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 15:45:57 2022, mtime=Tue Mar 8 15:45:57 2022, atime=Fri Aug 12 00:44:16 2022, length=2221348, window=hide

Category:	dropped
Size (bytes):	1104
Entropy (8bit):	4.5690329495881326
Encrypted:	false
SSDEEP:	12:8ogc5gXg/XAlCPCHaXNBQtB/SxXX+WNzkcfY5iO0OicvbZ16B789jH0IDtZ3YilR:8p8/XT9SUnzXZZe11C89dDv3qtu7D
MD5:	EAEB40053AC6C63FF2B4BD2DD421EFE3
SHA1:	FB30BEA503F379C7E27031786A0E603C86261760
SHA-256:	423C06D6C7C35343CF7BB8BBC69B38318BBFD001E66F3CE373BDABD382474826
SHA-512:	DDA8C88BCA7C42D587ABFAD76C7E5238E4258709D18697718AC8B35231AE37EE539242949B02BD9A5287AF9587C7DDD2DB1F17A1E72F2E662B9D77DE04EF54C7
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...../..3.../..3.....$.!.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.$.!..U.. .VALLIA~1.DOC..n.....hT..hT..*...r....'.....v.a.l.l.i.a.n.t...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\960781\Users.user\Desktop\valliant.document.08.11.2022.doc.7.....\....\....\....\....\....\.D.e.s.k.t.o.p.\.v.a.l.l.i.a.n.t...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...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:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
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\~$lliant.document.08.11.2022.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:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993464543538008
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:	valliant.document.08.11.2022.doc
File size:	2316502
MD5:	cadb9d5ed47b8df81a2addefed302a03
SHA1:	f7197fa991510f99f25af2b502c40d3b48d1abbc
SHA256:	9cb01729327bd958e32aa9481d5a81303627ab7a59b9ae134fb6600ef4e5b680
SHA512:	1b5ed9721c8d1aed9d09a850cb43afd6d756bbf6957ca6d8321c1fb5ea89a88a448f0aaa60348a70e30eda299c554619961c89b12888ea2ad6a6a5d058a54b07
SSDEEP:	49152:7t3L6IYFlSbzCFelOb0h5CZTsXG97qRbET6DLZ6dGbrG5j:BPYYgelO9T6G97qVg6DLZ6dGbyh
TLSH:	6DB533ED89E8E561F1433E32380557F3A45410D6EA5AC84A30C6FFC197962BB36E4F92
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/682606/sample/valliant.document.08.11.2022.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: 2826

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2826
Data ASCII:	. . A t t r i b u t . e V B _ N a m . e = " T h i . s D o c u m e n . t " . . . B a s . . 1 N o r m a l . . . V G l o b a l ! . S p a c . l F a . l s e . J C r e a . t a b l . . P r e d e c l a . . I d . . # T r u . " E x p . o s e . . T e m p . l a t e D e r i . v . $ C u s t o m l i z C . P . . . . . D . ? P t r S a . f e F u n c t . i o n > . . . . L . i b " u s e r . 3 2 " A l i a . s " S e t T i . m e r " (B y 8 V a l . . . . A s L o n g . , ... 3 . 9 . .
Data Raw:	01 fa 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: 369

General

Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	369
Entropy:	5.261233037013654
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 8 B 8 0 C 6 E 6 - B 7 5 8 - 4 1 8 F - A 2 4 D - 0 6 C 5 2 D 3 9 3 F 8 5 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 5 0 7 D 9 E 6 D B E F D F E F D F E F D F E F D F " . . D P B = " 0 A 0 8 D 6 E 1 D A E 2 D A E 2 D A " . . G C = " 0 F 0 D D 3 E C D D F 4 E 3 F 5 E 3 F 5 1 C " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 38 42 38 30 43 36 45 36 2d 42 37 35 38 2d 34 31 38 46 2d 41 32 34 44 2d 30 36 43 35 32 44 33 39 33 46 38 35 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 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 . 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	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5100
Entropy:	1.9259173726592043
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . " . . . . q . . . . A . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . `) . . . .
Data Raw:	72 55 40 04 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 22 00 1f 00 00 00 00 00 01 00 01 00 00 00 01 00 71 07 00 00 00 00 00 00 00 00 00 00 a1 07 00 00 00 00 00 00 00 00 00 00 d1 07

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 2724	
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.7004238887086345
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . ` . . . . . . . . . . . . . . . p . . . . . . . . . . . . . . . . . ! . . . . . . . . . A . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ` . . . . , . . p . . . . A . . . . a . . . . C P . . . . \\ . . p
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 60 00 c1 08 00 00 00 00 00 00 00 00 00 00 00 00 00 04 70 10 00 fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 486	
General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	486
Entropy:	6.3067050501427175
Base64 Encoded:	True

General	
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . @ d - . . . " . < . . . . r s t d o . l e > . . s . t . . d . o . l . e . (. . h . . ^ . . * \ \ . G { 0 0 0 2 0 4 3 0 - . . . . C . . . . . 4 6 } # 2 . 0 # . 0 # C : \ \ W i n . d o w s \ \ s y s @ t e m 3 2 \ \ . e 2 . . t l b # O L E . A u t o m a t . i o n . E N o r (m a l E N C r . m . a F . . c E C . . . . . m . ! O f f i c g O . f . i . c g . . g 2 D F 8 D 0 . 4 C - 5 B F A -
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 d3 40 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 18:45:10.985697985 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:45:11.089004993 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 18:45:11.089196920 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:45:11.089660883 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:45:11.192759991 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 18:45:11.210047960 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 18:45:11.210264921 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:45:16.215359926 CEST	80	49173	45.8.146.139	192.168.2.22
Aug 11, 2022 18:45:16.215564966 CEST	49173	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	49173	45.8.146.139	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 11, 2022 18:45:11.089660883 CEST	0	OUT	GET /fhfty/SKWR8YXON-RX9R4781JWMO3UUH0NGDBO/-f 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 18:45:11.210047960 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 16:45:11 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 2d 66 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 "-f" was not found on this server. </body></html>

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 1540, Parent PID: 576

General

Target ID:	0
Start time:	18:44:17
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:	0x13f4b0000
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	6E162B14	CreateDirectoryA

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 Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E4DA0EB	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E1BA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E1BA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E1BA5E3	RegCreateKeyExA

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