ID: 682577
Sample Name: airequipmentcorp-doc-08.11.2022.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:13:43
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

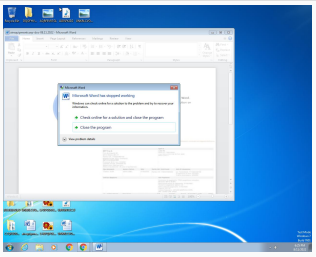
Windows Analysis Report

airequipmentcorp-doc-08.11.2022.doc

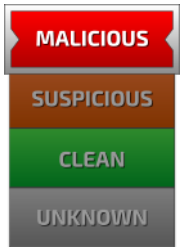
Overview

General Information

Sample Name:	airequipmentcorp-doc-08.11.2022.doc
Analysis ID:	682577
MD5:	84904f679048e4..
SHA1:	7e23ee02e2543e.
SHA256:	78c296d80214d8..
Tags:	doc IcedID
Infos:	



Detection

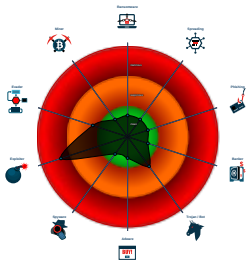


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2492 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)

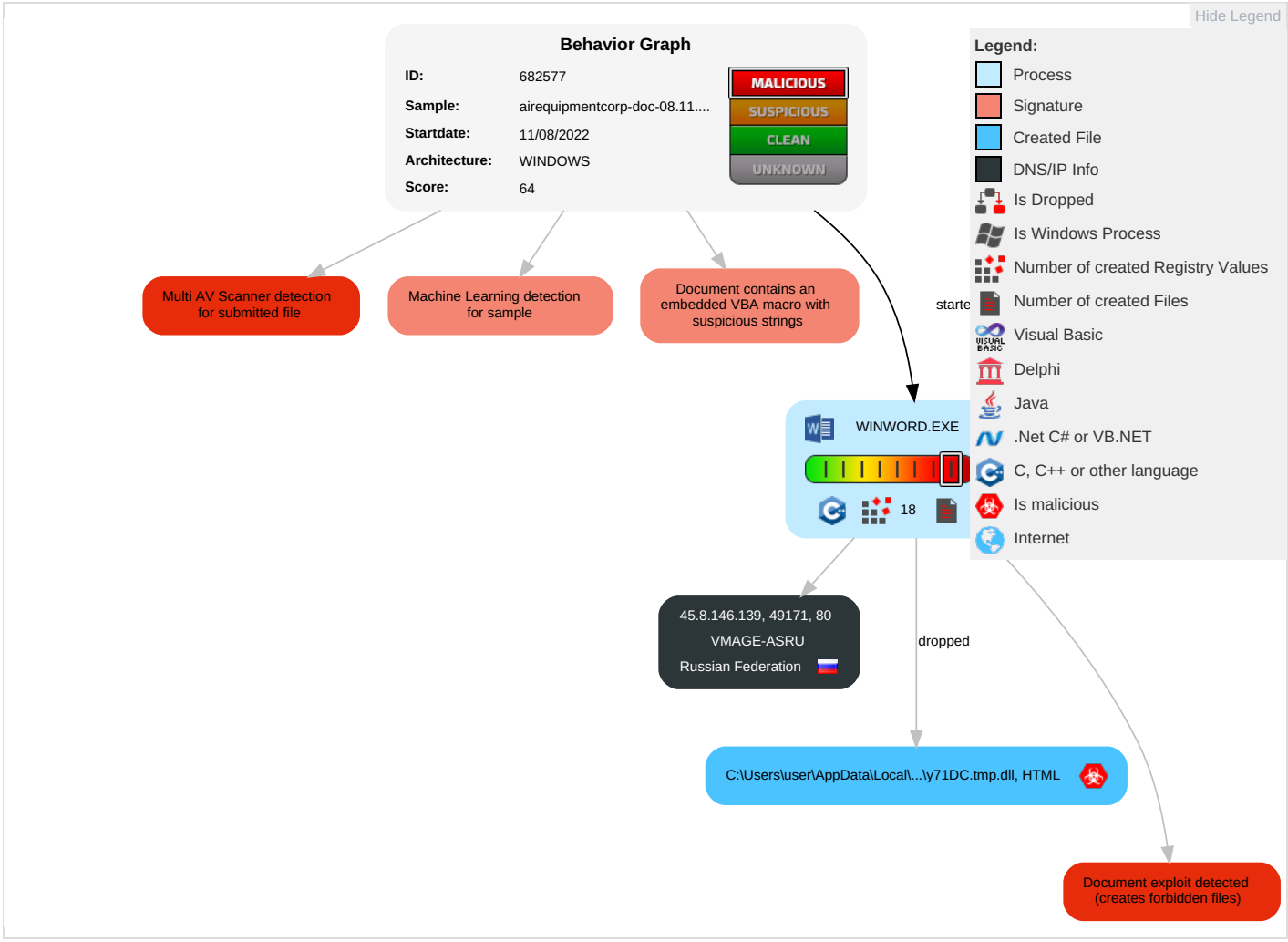
System Summary

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

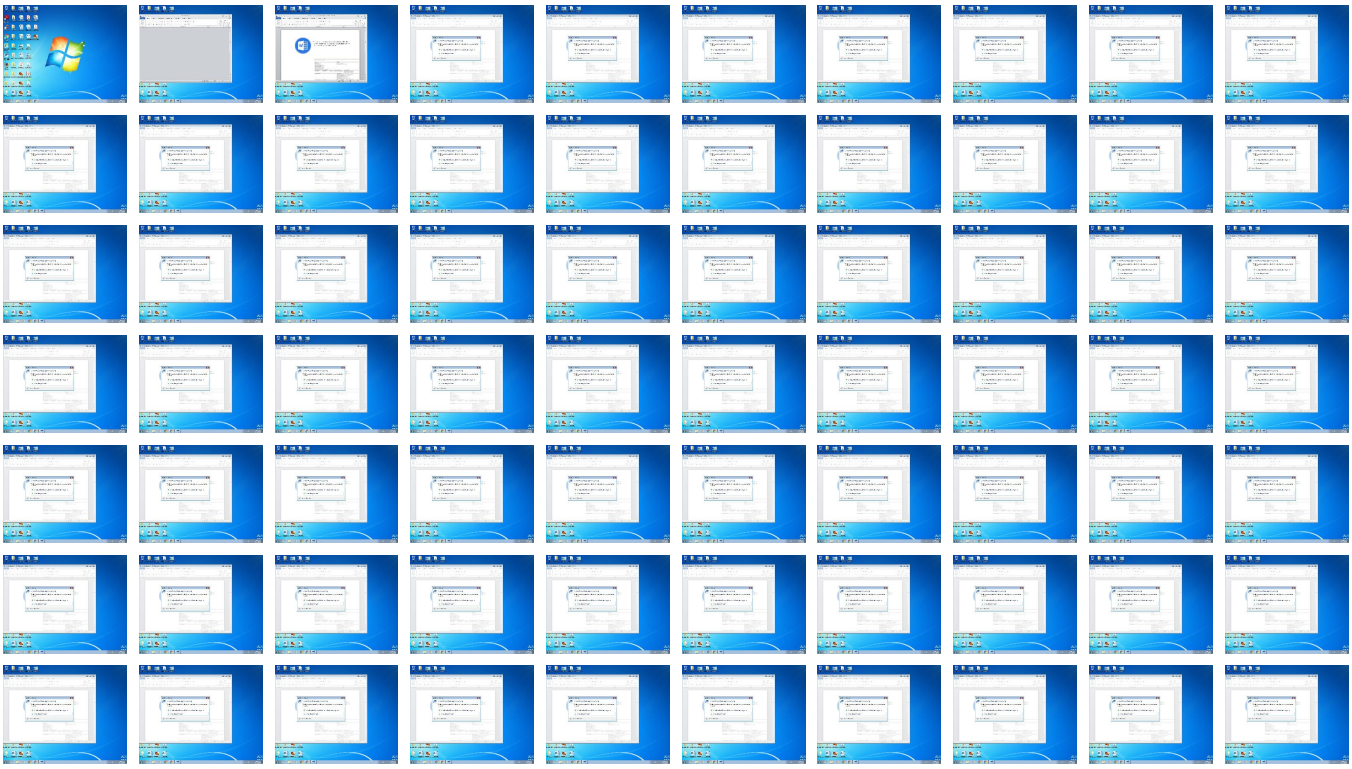
Behavior Graph

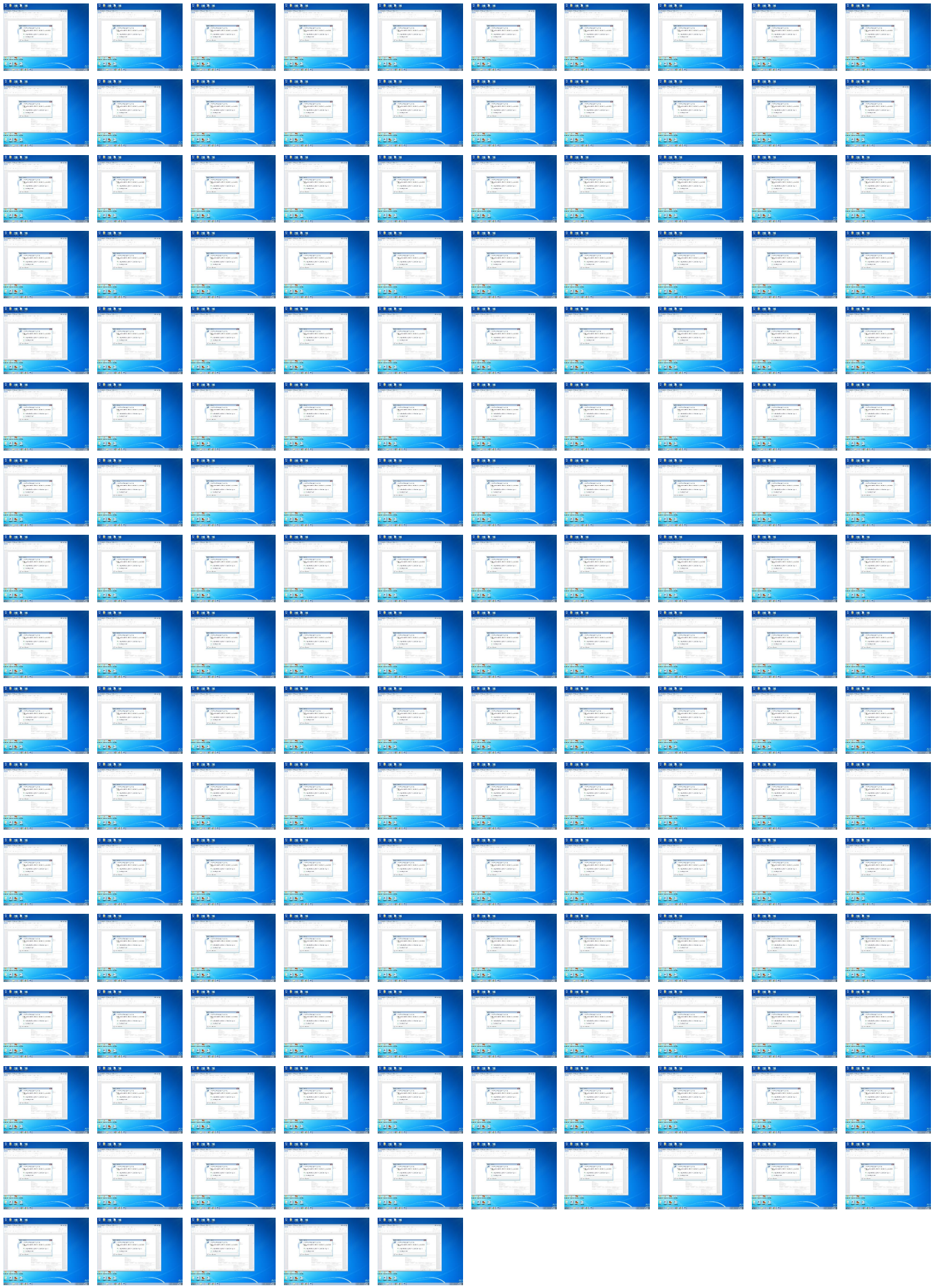


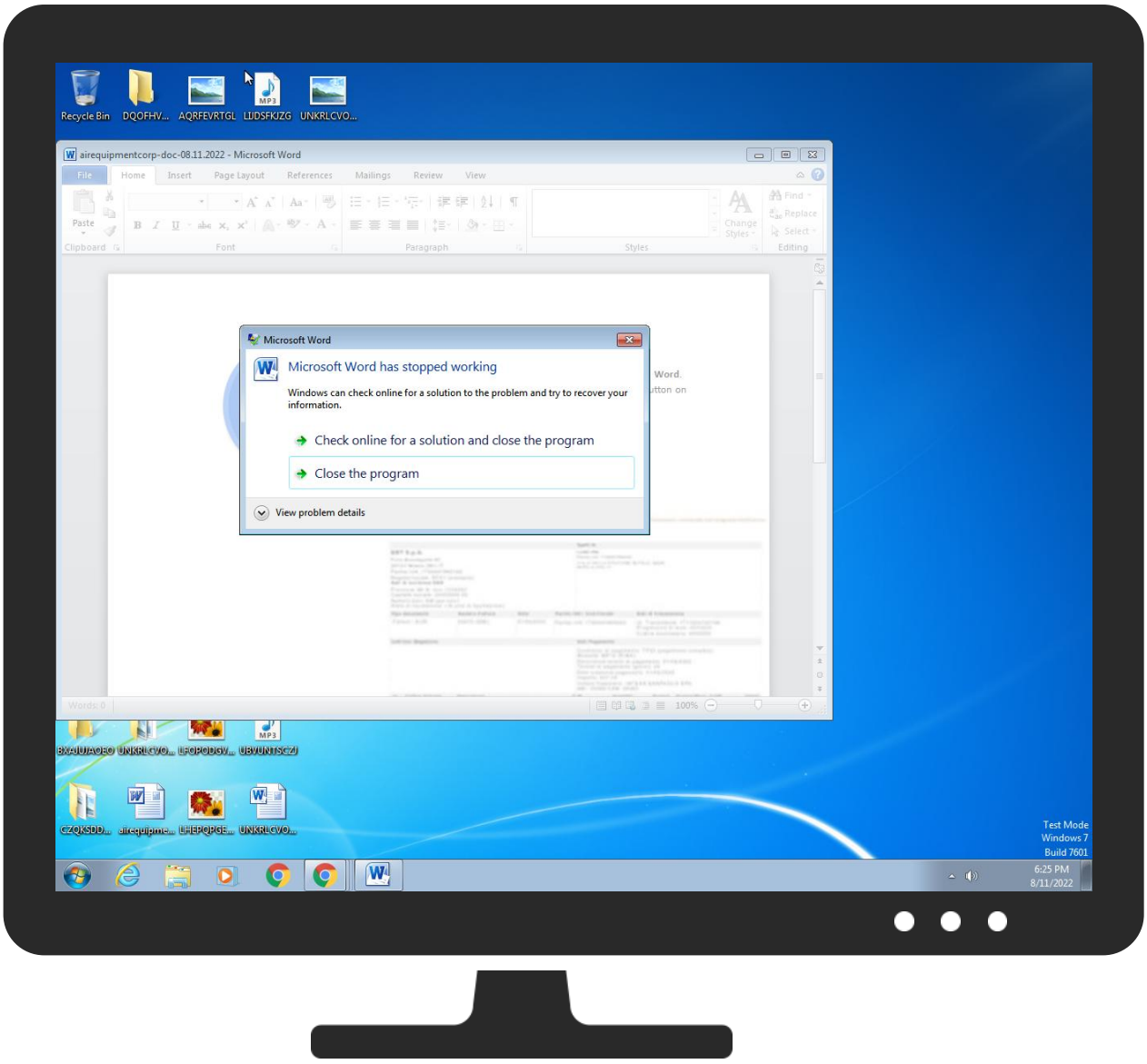
Screenshots

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
airequipmentcorp-doc-08.11.2022.doc	25%	Virustotal		Browse
airequipmentcorp-doc-08.11.2022.doc	15%	ReversingLabs	Script-Macro.Trojan.Amphitryon	
airequipmentcorp-doc-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/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/rm	0%	Avira URL Cloud	safe	

Domains and IPs

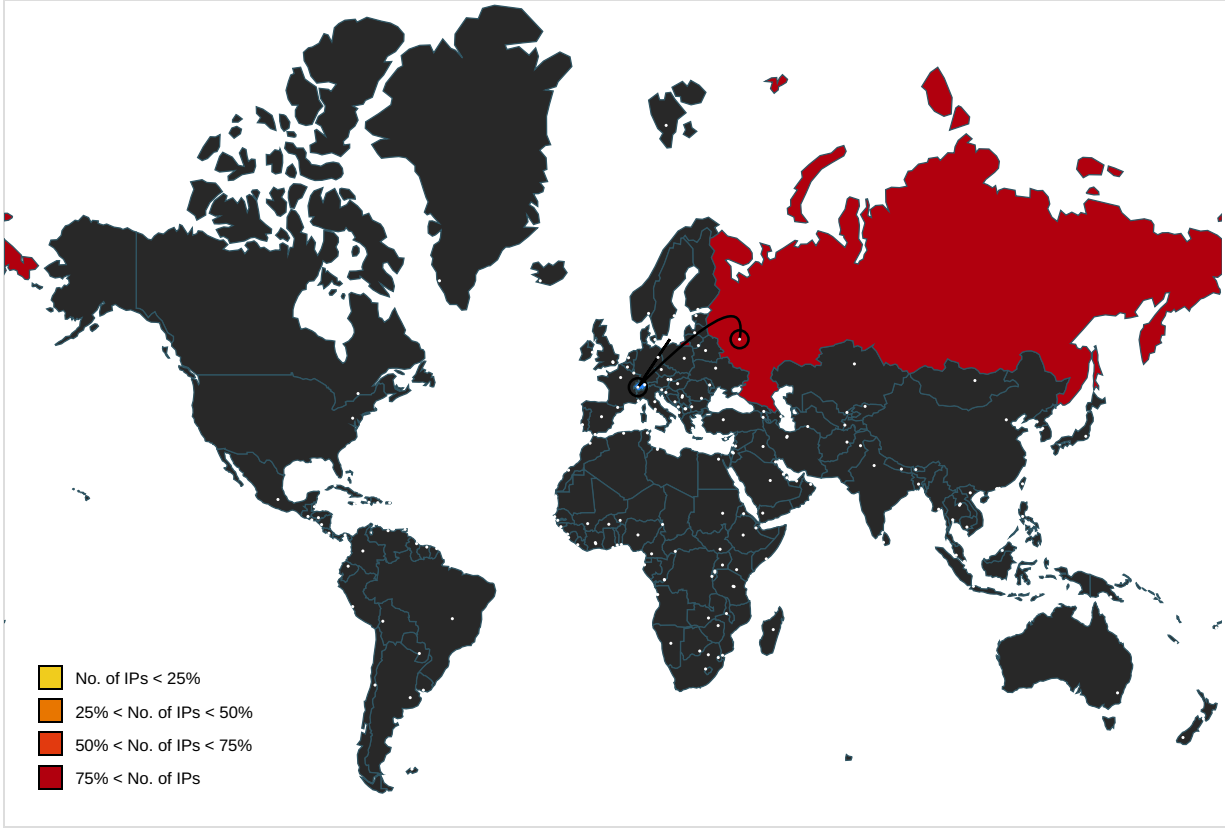
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.8.146.139/fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/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:	682577
Start date and time:	2022-08-11 18:13:43 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	airequipmentcorp-doc-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)
Run name:	Without Instrumentation
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 • 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\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:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C488076 3
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\y71DC.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:	02E47727BE33B93C4CA538A0E089720C0AC6D7CDC758216ECE0AD3380A75C151D9E2C6BA66A564209E3AC750720CBD3E415FA202ADE20852785D507C488076 3
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\airequipmentcorp-doc-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 15:45:53 2022, mtime=Tue Mar 8 15:45:53 2022, atime=Fri Aug 12 00:16:13 2022, length=2297841, window=hide
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	4.568111842563389
Encrypted:	false
SSDEEP:	12:8KSzSsbgXg/XAlCPCHaXRBktB/eLX+WdYW/xgi2LGejuicvbLysKX9sxLG8DtZ3k:8K3K/XThOMwW/xfKJeKsM9KDv3qau7D
MD5:	6F6ECFC265C7691AF267B206BB854DEB
SHA1:	FADA7B7607D69B87CCA7921ABFCB3405FB746C59
SHA-256:	93AEC371E303B4A3F9C4C07F0F3C4DD0B09DD13B9C3006E2AA75E64D16E7721B
SHA-512:	F64C52976F033DDC4DA4C82C4003377B01F635D185189E650F0B537B2DDE9E1DC9B06DEFCD53B1268D7DAFCEEF3C8019FB783E8BE250268A12B0E0F561E80C 9E
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.. .AIREQU~1.DOC..t.....hT..hT..*...r.....'.....a.i.r.e.q.u.i.p.m.e.n.t.c.o.r.p.-.d.o.c.-.0.8...1.1...2.0.2.2...d.o.c.....-...8...[.....?J.... ..C:\Users\..#.....\\179605\Users.user\Desktop\airequipmentcorp-doc-08.11.2022.doc.:.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.i.r.e.q.u.i.p.m.e.n.t.c.o.r.p.-.d.o.c.-.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

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):	113
Entropy (8bit):	4.790918623838269
Encrypted:	false
SSDEEP:	3:bDuMJlcMQJM3aBYUULX9omX1QM3aBYUULX9ov:bC3J+LX9Y+LX9y
MD5:	FABCBFCDEE2E5C7BCD854D1758F6218D
SHA1:	6A00305F129D1A8D869B57A4029190C7514EC1CD
SHA-256:	479B8AA7CFCEF33DDADE106F1D5250BA2EA30DF81C166717AB75851E72F1053E
SHA-512:	4771DCF03B0BF31070EE0637151037C9D2A7CB5073074EB5743BF907E355D7E7763F67068C8C2EB2B90E1B0EA9ECBFE84E5449126A3FD6819189516F4F41284D
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..airequipmentcorp-doc-08.11.2022.LNK=0..[doc]..airequipmentcorp-doc-08.11.2022.LNK=0..

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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
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\~$requipmentcorp-doc-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:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
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):	7.993807361796733

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:	airequipmentcorp-doc-08.11.2022.doc
File size:	2297841
MD5:	84904f679048e45c43210c22f8fcc5df
SHA1:	7e23ee02e2543e51a2ad97b2ede96c441d34e6eb
SHA256:	78c296d80214d887820a3c55bc06fbc42b17db90fb01aef0766365b383f1e7f1
SHA512:	c7f757c4b357b72f8edc9988ef99dd73b2d0fb9c48f928a3d806c57fbc168b8d2d141a625a5ce76a4c7a6533708984d200031bc56d44b6d756e512cfd823b3d7
SSDEEP:	49152:tqI9FlNmHCQkEV8Uxd938Vx8Z3rm06VNN9hTobO3b1:4I9F3miQkimVi3rD6VP4aB
TLSH:	F8B53302D0155771C5F1C8F98C5AA1B842B8D2321521EE5F4B3CB81ACBBDDCA7B85ADE
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.....hI.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/682577/sample/airequipmentcorp-doc-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: 2740

General

Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2740
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 V a l . . . . . A s L o n g , , { . . . . . , . .) .
Data Raw:	01 bc 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

General	
Stream Size:	369
Entropy:	5.245272756909884
Base64 Encoded:	True
Data ASCII:	I D = " { E F 2 1 A C D 1 - 0 7 C 6 - 4 1 0 B - 8 1 6 A - F 3 5 B E 5 6 2 A 9 A 6 } " . . 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 = " F 5 F 7 1 8 1 1 F 8 0 2 F C 0 2 F C 0 2 F C 0 2 F C " . . D P B = " E A E 8 0 7 2 0 F D 2 1 F D 2 1 F D " . . G C = " D F D D 3 2 3 F D 2 C 1 C 6 C 2 C 6 C 2 3 9 " . . . . [H o s t E x t e n d e r I n f
Data Raw:	49 44 3d 22 7b 45 46 32 31 41 43 44 31 2d 30 37 43 36 2d 34 31 30 42 2d 38 31 36 41 2d 46 33 35 42 45 35 36 32 41 39 41 36 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: 5116	
General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	5116
Entropy:	1.9229388656001654
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 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 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:	2.6943726453670886
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . x . . . . . ` . . . . . p . . . . . 1 . . . . . Q . . . . . q . . . . . ` . q . . . . . , . . p . . . . . 1 . . . . . Q . P . 1 . . . . . \ \ .
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 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 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 00 00 00 00 78 00 00 00 08 00 60 00 a1 08 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 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

General	
Entropy:	6.306571446096894
Base64 Encoded:	True
Data ASCII:	. . . . . 0 . . . . . H . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . R 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 dc 52 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 18:15:39.199373960 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:15:39.302838087 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 18:15:39.302978039 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:15:39.303560019 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:15:39.406869888 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 18:15:39.422107935 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 18:15:39.422405958 CEST	49171	80	192.168.2.22	45.8.146.139
Aug 11, 2022 18:15:44.426160097 CEST	80	49171	45.8.146.139	192.168.2.22
Aug 11, 2022 18:15:44.426340103 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 18:15:39.303560019 CEST	0	OUT	GET /fhfty/82PF9MOX9VRXL73GMCXOFE8AGP5ROGT8/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 18:15:39.422107935 CEST	1	IN	HTTP/1.1 200 OK Date: Thu, 11 Aug 2022 16:15:39 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: 2492, Parent PID: 576

General

Target ID:	0
Start time:	18:16:14
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:	0x13fda0000
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	6E1F2B14	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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E24A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E24A5E3	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