



ID: 682653 Sample Name: airdynefile08.11.22.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 19:56:47

Date: 11/08/2022

Version: 35.0.0 Citrine

#### **Table of Contents**

Vindows Analysis Report airdynefile08.11.22.doc  Overview General information Detection Signalures Classification Signalures Classification Wildows Configuration Yara Signatures Syrotts Signatures Syrott Signature Syrott Si	Table of Contents	
Overview General Information Decicion Signatures Classification Process The Process Signa Signatures Signa Signatures Signa Signatures Signa Signatures Signa Signatures Joe Sandbox Signatures Av Detection Mitra Attack Matrix Behavior Graph Size enshols Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unitial Sample Dropped Files Unitial Sample Dropped Files Unitial Sample Dropped Files Size enshols Size en	Windows Analysis Report airdynefile08.11.22.doc	4
Detection Signatures Classification Process Tree Malware Configuration Yara Signatures Signa Signatures Signa Signatures Signa Signatures Joe Sandbox Signatures Joe Sandbox Signatures AV Detection System Summary Mitter Allock Matrix Behavior Graph Screenshols Thombrais Behavior Graph Screenshols Thombrais Doupod Files Domains Doupod Files Domains URL3 Domains and IPS Contacted Domains URL3 Domains and IPS Contacted Domains Simulations Simulations Behavior and APIs Domains Simulations Behavior and APIs Dosains Dospoel Files Created / dropped Files Creat		
Signatures Cinastication Process Tree Maware Configuration Yara Signatures Signatures Signatures Signatures Signatures Joe Sandbox Signatures Joe Sandbox Signatures AV Detection System Summary Mittre Attack Matrix Behavior Graph Screenshots Trumbnals Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unitial Unit	General Information	
Ciasafication Process Tree Malware Configuration Yara Signatures Signa Signatures Signa Signatures Joe Sandbox Signatures AV Detection System Summary Mitre Attack Matrix Behavior Graph Screenshots Thumbnalis Anthivirus, Machine Learning and Genetic Malware Detection Initial Sample Toropped Files Unpacked PE Files Unp		
Process Tree Malware Configuration Yara Signatures Signa Signatures Joe Sandbox Signatures AV Detection AV Detection Thumbraic Screenshots Thumbraic Screenshots Thumbraic Marbirus, Machine Learning and Genetic Malware Detection Initial Screenshots Thumbraic Unpacked PE File Domains Untla Domains and IPS Contacted Domains World Map of Contacted IPS Pates Services Service	,.Y	
Makware Configuration Yara Signatures Sigma Signatures Sigma Signatures Joe Sandbox Signatures AV Detection System Summary White Attack Matrix Mitter Attack Matrix Behavior Graph Screenshore Trumbnais Antivirus, Machine Learning and Genetic Malware Detection Initial Sampie Dropped Flee Dropped Flee Dropped Flee Domains and IPs Contacted Domains World Map of Contacted IPs Pute-IPs Contacted Domains World Map of Contacted IPs Pute-IPs Contacted Domains Simulations Behavior and APs Behavior and APs Behavior and APs Behavior and APs Contacted IPs Pute-IPs Contacted Institute Inst		
Yara Signatures Signa Signatures Sonot Signatures AV Detection System Summary Mitre Attack Matrix Behavior Graph Screenshots Thumbrouls Antivirus, Machine Learning and Genetic Malware Detection initial Sample Dropped Files Unpacked FE Files Domains URLs URLs Domains and IPs Contacted Domains World Map of Contacted IPs General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPs Domains Colleges Files Domains Colleges Files		
Signa Signatures Joe Sandbox Signatures AV Deleticinn System Summary Mitre Attack Matrix Behavior Graph Screenshots Thermhalis Anthrivins Machine Learning and Genetic Malware Detection Institution Sample Diopped Files Unpacked Fe Files Openation Sample United Sample Diopped Files Unpacked Fe Files Openation Sample Domains and IPs Contacted Domains World Map of Contacted IPs Profess IPs Contacted Domains Simulations Contacted IPs Profess Simulations Simulations Simulations Simulations Simulations Simulations Simulations Contacted IPs Profess Simulations Contacted Insurance Contact		
Snort Signatures AV Detection System Summary Mitre AttRck Matrix Behavior Graph Screenshots Thombrails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Unpacked PE Files Domains Unpacked PE Files Domains Unitial Manager Unitial Some Unitial Sample Unitial Some Selevitivi and APIS Obermains World Map of Contacted IPIs Paule IPIs General Information Warnings Simulations Behavior and APIS Joe Sandbox View / Context IPIs Domains ASNs JAS Trigorprints Dropped Files Created / dr		
Joe Sandbox Signatures AV Detection System Summary Mittre Attack Matrix Behavior Graph Screenshots Thumbnalis Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked FE F		
AV Detection System Summary Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnails Antivirus, Machine Learning and Genetic Mahware Detection Initial Sample Dropped Files Unpacked FE Files Domains URLs URLs URLs URLs URLs URLs URLs URL	_ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
System Summary Mitre Attack Matrix Behavior Graph Screenshots Thumbrails Antivirus, Machine Learning and Genetic Malware Detection initial Sample Dropped Files Units, Dromains and IPS Contacted Domains World Map of Contacted IPs Pate: Ps General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPs Domains ASNs ASNs ASNs ASNs ASNs ASNs ASNs ASN		
Mitre Att&ck Matrix Behavior Graph Screenshots Thumbnalls Antivirus, Machine Learning and Genetic Malware Detection initial sample Dropped Flies Unpacked FE Files Domains Unpacked FE Files Domains World Map of Contacted IPs General Information Warnings Simulations Behavior and APis, Doe Sandbox View / Context IPs Domains Domains Domains Simulations Behavior and APis, Dee Sandbox View / Context IPs Consected Domains Contacted Information Warnings Simulations Behavior and APis, Doe Sandbox View / Context IPs Contacted Information Contacted Information Warnings Simulations Contacted Information Warnings Simulations Endowor and APis, Doe Sandbox View / Context IPs Contacted Information Contacted Information Warnings Contacted Information		
ScreenShots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs URLs Domains and IPS Contacted Domains World Map of Contacted IPS Palis IPS General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASNs JA3 Fingerprints Dropped Files Created / dropped	, , , , , , , , , , , , , , , , , , , ,	
ScreenShots Thumbnails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs URLs Domains and IPS Contacted Domains World Map of Contacted IPS Palis IPS General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASNs JA3 Fingerprints Dropped Files Created / dropped	Behavior Graph	
Thumbhails Antivirus, Machine Learning and Genetic Malware Detection Initial Sample Dropped Files Unpacked PE Files Domains URLs  Contacted Domains  Warnings Simulations General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASNs JAS Pringerprints Dropped Files Created / dropped Files Created / dropped Files Created / dropped Files CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 1. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 2. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 3. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 3. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 4. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.MSO\SADBDEF.png 5. CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.Word-WRS(0291843-050C-46A7-AEE-876A98012E3A).Im CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.Word-WRS(0291843-050C-46A7-AEE-876A98012E3A).Im CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.Word-WRS(0291843-050C-46A7-AEE-876A98012E3A).Im CutsersuserAppDatatio.caliMicrosoftWindows1Temporary Internet Files\Content.Word-WRS(0291843-050C-46A7-AEE-876A98012E3A).Im CutsersuserAppDatatio.caliming\Contents\Conte		
Initial Sample Dropped Files Unpacked PE Files Domains URLs Domains and IPs Contacted Domains Warning Simulations Behavior and APIs Oeneral Information Warnings Simulations Behavior and APIs De Sandbox View / Context IPs Domains ASNs JAS Fingerprins Domains ASNs JAS Fingerprins Domains ASNs Contacted Domains ASNs JAS Fingerprins Domains JAS Fingerprins JAS	Thumbnails	
Diopped Files Domains URLs Domains and IPS Contacted Domains World Map of Contacted IPS Public IPP General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ANNs Joe Sandbox View / Context IPS Domains ANNs ANNs ANNs ANNs ANNs ANNs ANNs AN	Antivirus, Machine Learning and Genetic Malware Detection	
Unpacked PE Files Domains URLs Domains and IPS Contacted Domains World Map of Contacted IPS Public IPS General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASNS JA3 Fingerprints Dropped Files Created /	Initial Sample	
Domains and IPs Contacted Domains World Map of Contacted IPs rubio its General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPs Domains ASNs Joe Sandbox View / Context IPs Domains ASNs Joe Sandbox View / Context IPs Contacted / dropped Files Created / dropped F		
URLS Domains and IPS Contacted Domains World Map of Contacted IPS Note of Contacted IPS Simulations Behavior and APIS Joe Sandbox View / Context IPS Domains ASNS JA3 Fingerprints Dropped Files Created / dropped Fil		
Contacted Domains World Map of Contacted IPS Public IPs General Information Warnings Simulations Behavior and APIS Joe Sandbox View / Context IPS Domains ASNs JA3 Fingerprints Dropped Files Cruted / dropped Files Cruter-App DatalLocalMicrosoftWindows\Temporary Internet Files\Content.MSO\5AB8DEF.png 1 Cruter-App DatalLocalMicrosoftWindows\Temporary Internet Files\Content.MSO\5B880826.png 1 Cruter-App DatalLocalMicrosoftWindows\Temporary Internet Files\Content.World-WRF(A1B0D/TC-F7EF-4F37-9130-C1Users\underser-App DatalLocalMicrosoftWindows\Temporary Internet Files\Content.World-WRF(5092)848-D50C-46A7-AEE5-876A98012E3A\temporary Internet Files\Content.World-WRS(5092)848-D50C-46A7-AEE5-876A98012E3A\temporary Internet Files\Content.World-WRS(5092)8		
Workings  General Information  Warnings  Simulations Behavior and APIs Joe Sandbox View / Context  IPs Domains ASNs JAS Fingerprints Dropped Files  C-Reated / dropped Files	Domains and IPs	
Felible Information  Warnings  Simulations Behavior and APIs  Joe Sandbox View / Context  IPS  Domains  ASNs  JA3 Fingerprints  Dropped Files  Created / dropped Files  Streams with VPA  VPA in Files Files Files Files Eige Side Side with role to the transverse, Stream Size 7  Stream Files Files Content Word-War-Files Files Files Files Files Files Files Content Word-War-Files Files	Contacted Domains	
General Information Warnings Simulations Behavior and APIs Joe Sandbox View / Context IPP Domains ASNs JA3 Fingerprints Dropped Files Created / droppe		
Simulations Behavior and APIs Joe Sandbox View / Context IPS Domains ASNs JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files Criticers with Appolatation and Microsoft Windows Temporary Internet Files Content. MSO ISAB DEF. png Criticers with Appolatation and Microsoft Windows Temporary Internet Files Content. MSO ISAB DEF. png Criticers with Appolatation and Microsoft Windows Temporary Internet Files Content. MSO ISAB DEF. png Criticers with Appolatation and Microsoft Windows Temporary Internet Files Content. Word - WRF (A1B DD TEC TFE - 4F37-9130-CDF90 AC 285 CB). mp Criticers with Appolatation and Microsoft Windows Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - WRS (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - Wrs (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - Wrs (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - Wrs (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - Wrs (99291B43-D50C-46A7-AEE5-876A98012E3A). tm Criticers with Appolatation and Temporary Internet Files Content. Word - Word - Wrs (99291B43-D50C-46A		
Simulations Behavior and APIs Joe Sandbox View / Context  IPs Domains ASNs JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files C:\Users\user\AppData\user\AppData\user\appData\undow\appData\user\appData\user\appData\user\appData\user\appData\undow\appData\undow\appData\undow\appData\undow\appData\undow\		
Behavior and APIS Joe Sandbox View / Context IPS Domains ASNs JA3 Fingerprints Dropped Files Created / dropped Files Crulesriuser/AppDatalLocalMicrosoft(Windows\Temporary Internet Files\Content.MSO\SAD8DEF.png 1.1 C:\Users\user\user\user\uper\uper\uper\uper\uper\uper\uper\up	,	
Joe Sandbox View / Context IPs Domains ASNs JA3 Fingerprints Dropped Files Created / dropped Files Created / dropped Files Created / dropped Files Created / dropped Files Crusers/suser/AppDatalLocalMicrosoft/Windows\Temporary Internet Files\Content.MSO\SADBDEF.png 1. C:\Users\user\user\under\u	,	
IPS Domains ASNs JA3 Fingerprints Dropped Files Created / dropped Files Crusers\user\u00e4appData\u00e4\u00e		
ASNs JA3 Fingerprints Dropped Files  Created / dropped Files  C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.MSO\5AD8DEF.png .1 C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.MSO\5AD8DEF.png .1 C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.MSO\5AD8DEF.png .1 C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.Word\-WRS\{09291B43-D5C-46A7-AEE5-876A98012E3A}.tm C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.Word\-WRS\{09291B43-D5C-46A7-AEE5-876A98012E3A}.tm C:Users'user'AppDatalLocalMicrosoftWindows\Temporary Internet Files\Content.Word\-WRS\{09291B43-D5C-46A7-AEE5-876A98012E3A}.tm C:Users'user'AppDatalLocalMicrosoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-1E056839B7F47}.tmp .1 C:Users'user'AppDatalLocalMicrosoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-1E056839B7F47}.tmp .1 C:Users'user\AppDatal\Coal\Temp\-D=176F4133B71F1140.TMP .1 C:Users'user\AppDatal\Roaming\Microsoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-161}.tm .1 C:Users'user\AppDatal\Roaming\Microsoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-161}.tm .1 C:Users'user\AppDatal\Roaming\Microsoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-161}.tm .1 C:Users'user\AppDatal\Roaming\Microsoft\Office\Recentlindry\temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-181}.tm .1 C:Users'user\AppDatal\Roaming\Microsoft\Office\Recentlindry\temporary Internet Files\Content\Uniternet Internet Fi		
JA3 Fingerprints Dropped Files Created / dropped Files C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AB8EF.png C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png 1:\C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png 1:\C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRF\{A1B0DTEC-FTEF-4F37-9130-CDF90AC285CB}.tmp 1:\C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRS\{09291B43-D50C-46A7-AEE5-876A98012E3A}.tm C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRS\{09291B43-D50C-46A7-AEE5-876A98012E3A}.tm C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRS\{6194CBA3-C75A-48F7-92FA-105C8398F747\temporary\tempo		
Created / dropped Files  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.MSO\5AD8DEF.png  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png  1. C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.Word\~WRF\(AB0DTEC-F7EF-4F37-9130-CDF90AC285CB\).tmp  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.Word\~WRF\(AB0DTEC-F7EF-4F37-9130-CDF90AC285CB\).tmp  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.Word\~WRS\(9291843-D50C-46A7-AEE5-876A98012E3A\).tm  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.Word\~WRS\(6194CBA3-C75A-48F7-92FA-105C83987F47\).tmp  C:\Users\user\AppDatal\uca\lMicrosoft\Windows\Temporary Internet Files\Content.Word\~WRS\(6194CBA3-C75A-48F7-92FA-105C83987F47\).tmp  C:\Users\user\AppDatal\uca\lming\Microsoft\Office\Recent\airdynefile08.11.22.LnK  C:\Users\user\AppDatal\ucae\AppDatal\ucae\ming\Microsoft\Office\Recent\airdynefile08.11.22.LnK  C:\Users\user\AppDatal\ucae\AppDatal\ucae\ming\Microsoft\Office\Recent\airdynefile08.11.22.LnK  1. C:\Users\user\AppDatal\ucae\AppDatal\ucae\ming\Microsoft\Uperoof\under\u		
Created / dropped Files C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\SABBDEF.png C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\SB980826.png C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSo\SB980826.png C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{AIBOD7EC-F7EF-4F37-9130-CDF90AC285CB}.tmp C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS\(99291843-D50C-46A7-AEE5-876A9B012E3A\).tm C:Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS\(6194CBA3-C75A-48F7-92FA-105C808987F47\).tm C:Users\user\AppData\Local\Temp\-DF176F4133871F1140.TMP C:Users\user\AppData\Roaming\Microsoft\Office\Recent\under\		
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.MSO\SAD8DEF,prg C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.MSO\Sp80826.png C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF(A180D7EC-F7EF-4F37-9130-CDF90AC285C8}.tmp C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF(6194D83-D50C-46A7-AEE5-876A98012E3A}.tm C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS(6194CBA3-C75A-48F7-92FA-ID-105C839B7F47).tmp C:\Users\user\AppData\Loca\User\User\User\User\User\User\User\User		
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.MSO\58980826,png C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{A180D7EC-F7EF-4F37-9130-CDF90AC285CB}.tmp C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.tmp C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.tmp C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp C:\Users\user\AppData\Roaming\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp C:\Users\user\AppData\Roaming\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp C:\Users\user\AppData\Roaming\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C8-E05-E05-E05-E05-E05-E05-E05-E05-E05-E05		1
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.  C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp  C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP  C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK  C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK  C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK  C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK  C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK  C:\Users\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En\Odday.dot  C:\Users\user\Desktop\~\$rdynefile08.11.22.doc  1. Clusers\user\Desktop\~\$rdynefile08.11.22.doc  1. Clusers\user\Desktop\\$ file Info  General  General  General  OLE File 'noptpackage/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc*  miciacors  Streams with VBA  VBA File kame: 'Thebournert.ds, Stream Size-2860  General  Ole File 'noptpackage/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc*  miciacors  Streams and PROJECT, File Type. ASCII text, with CRLF line terminators, Stream Size-365  Streams  Stream Path 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General  Stream Path: 'VBA/ 'SRP 2. File Type: data, Stream Size-214  General	C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png	
C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\—WRS\(99291B43-D50C-46A7-AEE5-876A9B012E3A\).tm C:\Users\user\AppData\Loca\Microsoft\Windows\Temporary Internet Files\Content.Word\—WRS\(6194CBA3-C75A-48F7-92FA-E05C839B7F47\).tmp C:\Users\user\AppData\Loca\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Loca\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\aird\overline{\text{Prop}}. C:\Users\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\Users\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\Users\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\Users\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\User\user\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\User\user\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\User\user\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\User\user\user\AppData\Roaming\Microsoft\Uproof\ExcludeDictionary\En0409.lex C:\User\user\user\AppData\Roaming\Microsoft\Uproof\Endalta\user\under\user\user\User\user\under\under\user\under\user\und		1
C:\Users\user\AppData\Loca\\Microsoft\Windows\Temporary Internet Files\Content.Word\-WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp C:\Users\user\AppData\Loca\\Temp\-DF176F4133B71F1140.TMP C:\Users\user\AppData\\Loca\\Temp\-DF176F4133B71F1140.TMP C:\Users\user\AppData\\Roaming\Microsoft\Office\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Office\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\user\AppData\\Roaming\Microsoft\Uffice\Recent\under\text{add} C:\Users\user\under\user\under\un		
C:\Users\user\AppData\Local\Temp\-DF176F4133B71F1140,TMP C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\under\und		
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\airdynefile08.11.22.LNK C:\Users\user\AppData\Roaming\Microsoft\Ufroof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\Ufroof\ExcludeDictionaryEN0409.lex C:\Users\user\Desktop\-\$rdynefile08.11.22.doc  Static File Info General General Gile Icon Static OLE Info General OLE File "topt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators Streams with VBA VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA File Name: ThisDocument.cls, Stream Size: 2860 General Streams Path: PROJECT, File Type: data, Stream Size: 41 General Streams Path: PROJECT, File Type: data, Stream Size: 41 General Stream Path: VBA_VBA_PROJECT, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General	E05C839B7F47).tmp	
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat C:\Users\user\AppData\Roaming\Microsoft\Templates\-\$\Normal.dotm C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\user\user\uper\uper\uper\uper\uper\uper\uper\up		
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm C:\Users\user\AppData\Roaming\Microsoft\UProoftExcludeDictionaryEN0409.lex C:\Users\user\Desktop\~\$rdynefile08.11.22.doc  Static File Info General File Icon Static OLE Info General OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators Streams with VBA VBA File Name: Thisbocument.ds, Stream Size: 2860 General VBA Code Streams Stream Path: VBOJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PBOJECT, File Type: data, Stream Size: 41 General Stream Path: VBA_VBA_PROJECT, File Type: data, Stream Size: 41 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2486 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2486 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2486 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2486 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2486 General Stream Path: VBA_GIR, File Type: data, Stream Size: 2486 General		
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex C:\Users\user\Desktop\-\\$rdynefile08.11.22.doc  Static File Info  General File Icon Static OLE Info  General OLE File "\pot\package/joesandbox\database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators Streams with VBA VBA File Name: Thisbocument.cls, Stream Size: 2860 General VBA Code Streams Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 385 General Stream Path: PROJECT, File Type: data, Stream Size: 41 General 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: data, Stream Size: 5108 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 486 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 486 General Stream Path: VBA_SRP_1, File Type: data, Stream Size: 486 General Stream Path: VBA_JGRP_1, File Type: data, Stream Size: 486 General Network Behavior		
Static File Info  General  File Icon  Static OLE Info  General  OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators  Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA Code  Streams Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECT, File Type: data, Stream Size: 41 General 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: data, Stream Size: 5108 General Stream Path: VBA_SRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General Stream Path: VBA_GRP_3. File Type: data, Stream Size: 2724 General	C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	1
General File Icon Static OLE Info General OLE File "lopt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators Streams with VBA VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA Code Streams Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECT, File Type: data, Stream Size: 41 General Stream Path: PROJECT, File Type: data, Stream Size: 41 General Stream Path: VBA/ VBA PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA/ SRP 2, File Type: data, Stream Size: 5108 General Stream Path: VBA/ SRP 3, File Type: data, Stream Size: 2724 General Stream Path: VBA/GIR, File Type: data, Stream Size: 2724 General Stream Path: VBA/GIR, File Type: data, Stream Size: 486 General Network Behavior		
File Icon  Static OLE Info  General  OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators  Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA Code  Streams  Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECTwwn, File Type: data, Stream Size: 41 General Stream Path: VBA/ yBA PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA/ SRP 2, File Type: data, Stream Size: 5108 General Stream Path: VBA/ SRP 3, File Type: data, Stream Size: 2724 General Stream Path: VBA/ SRP 3, File Type: data, Stream Size: 2786 General Stream Path: VBA/ SRP 3, File Type: data, Stream Size: 2866 General Stream Path: VBA/dir, File Type: data, Stream Size: 2866 General  Network Behavior		
Static OLE Info  General  OLE File "/ppt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators  Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA Code  Streams  Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: VBA/VBA PROJECT, File Type: data, Stream Size: 41 General Stream Path: VBA/VBA PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA/SRP 2, File Type: data, Stream Size: 5108 General Stream Path: VBA/SRP 3, File Type: data, Stream Size: 2724 General Stream Path: VBA/SRP 3, File Type: data, Stream Size: 2724 General Stream Path: VBA/Gir, File Type: data, Stream Size: 486 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General		
General  OLE File "lopt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc" Indicators  Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860 General VBA Code  Streams  Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General  Stream Path: PROJECTwm, File Type: data, Stream Size: 41 General  Stream Path: VBA_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General  Stream Path: VBA_SRP_2. File Type: data, Stream Size: 5108 General  Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General  Stream Path: VBA_JGRP_3, File Type: data, Stream Size: 2724 General		
Indicators  Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860  General  VBA Code  Streams  Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365  General  Stream Path: PROJECTwm, File Type: data, Stream Size: 41  General  Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7  General  Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108  General  Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724  General  Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724  General  Stream Path: VBA/dir, File Type: data, Stream Size: 486  General  Network Behavior		
Streams with VBA  VBA File Name: ThisDocument.cls, Stream Size: 2860  General  VBA Code  Streams  Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365  General  Stream Path: PROJECTwm, File Type: data, Stream Size: 41  General  Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7  General  Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108  General  Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724  General  Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724  General  Stream Path: VBA/_SRP_1, File Type: data, Stream Size: 2724  General  Stream Path: VBA/_SRP_1, File Type: data, Stream Size: 2724  General  Stream Path: VBA/Jir, File Type: data, Stream Size: 486  General  Network Behavior		
General VBA Code Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECTwm, File Type: data, Stream Size: 41 General Stream Path: VBA_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General Stream Path: VBA/Director Company Compan	~	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECTwm, File Type: data, Stream Size: 41 General Stream Path: VBA_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/GRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General Stream Path: VBA/Dir, File Type: data, Stream Size: 486 General		
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365 General Stream Path: PROJECTwm, File Type: data, Stream Size: 41 General Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General	VBA Code	
Stream Path: PROJECTwm, File Type: data, Stream Size: 41 General Stream Path: VBA_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA\_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA\_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA\/dir, File Type: data, Stream Size: 486 General Network Behavior	Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 365	
Stream Path: VBA_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7 General Stream Path: VBA_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General Network Behavior		
General Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108 General Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General  Network Behavior  1	General	
General Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724 General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General  Network Behavior  1	General	
General Stream Path: VBA/dir, File Type: data, Stream Size: 486 General  Network Behavior  1	General	
Network Behavior 1	General	
	General	

Statistics	15
System Behavior	16
Analysis Process: WINWORD.EXEPID: 2492, Parent PID: 576	16
General	16
File Activities	16
File Created	16
File Deleted	16
File Read	16
Registry Activities	16
Key Created	16
Key Value Created	17
Key Value Modified	18
Disassembly	22

#### **Windows Analysis Report**

airdynefile08.11.22.doc

#### **Overview**

#### **General Information**



#### Detection



#### Signatures



#### 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

Copyright Joe Security LLC 2022 Page 4 of 22

#### Joe Sandbox Signatures

#### **AV Detection**



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

#### **System Summary**

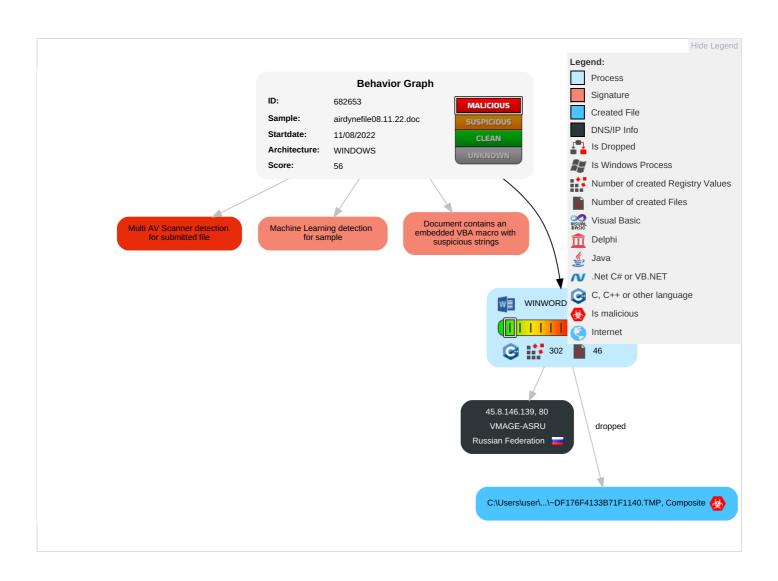


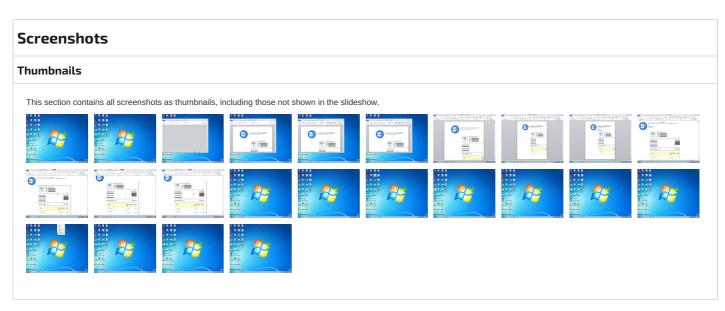
Document contains an embedded VBA macro with suspicious strings

Mitre	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 Interceptio n	Path Interceptio n	1 Masqueradi ng	OS Credential Dumping	File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	Exploitation for Client Execution	Boot or Logon Initializatio n Scripts	Boot or Logon Initializatio n Scripts	1 2 Scripting	LSASS Memory	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 Authorizati on	Device Lockout

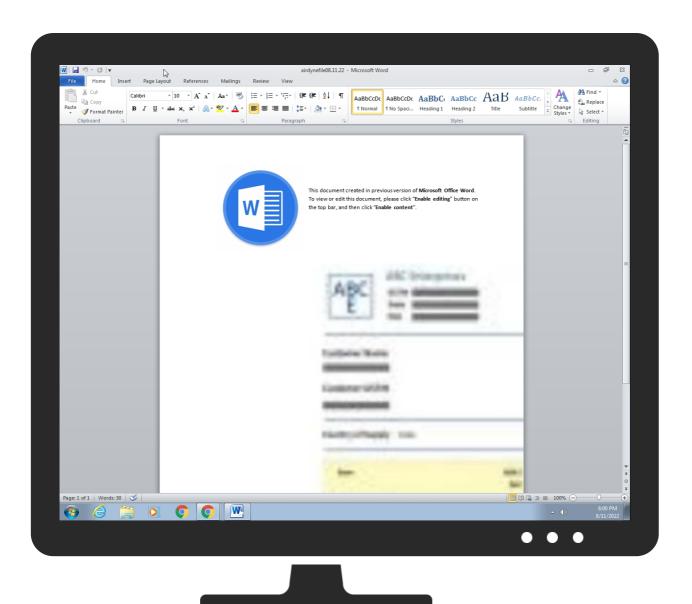
#### **Behavior Graph**

Copyright Joe Security LLC 2022 Page 5 of 22





Copyright Joe Security LLC 2022 Page 6 of 22



#### Antivirus, Machine Learning and Genetic Malware Detection **Initial Sample** Source Detection Scanner Label Link airdynefile08.11.22.doc 27% Virustotal Browse airdynefile08.11.22.doc 15% ReversingLabs Script-. Macro.Trojan.Amp hitryon airdynefile08.11.22.doc 100% Joe Sandbox ML **Dropped Files** Detection Scanner Label Link $C:\label{local-Templ-DF176F4133B71F1140.TMP} C:\label{local-Templ-DF176F4133B71F1140.TMP} The state of the$ 100% Joe Sandbox ML **Unpacked PE Files** No Antivirus matches

## Domains ⊘ No Antivirus matches

Copyright Joe Security LLC 2022 Page 7 of 22

**URLs** 

#### **Domains and IPs**

#### **Contacted Domains**

No contacted domains info



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:	682653
Start date and time:	2022-08-11 19:56:47 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	airdynefile08.11.22.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:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Copyright Joe Security LLC 2022 Page 8 of 22

Number of injected processes analysed:	0
Technologies:	<ul> <li>HCA enabled</li> <li>EGA enabled</li> <li>HDC enabled</li> <li>GSI enabled (VBA)</li> <li>AMSI enabled</li> </ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul> <li>Successful, ratio: 100%</li> <li>Number of executed functions: 0</li> <li>Number of non-executed functions: 0</li> </ul>
Cookbook Comments:	<ul> <li>Found application associated with file extension: .doc</li> <li>Adjust boot time</li> <li>Enable AMSI</li> <li>Found Word or Excel or PowerPoint or XPS Viewer</li> <li>Attach to Office via COM</li> <li>Scroll down</li> <li>Close Viewer</li> </ul>

#### Warnings

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

Joe Sandbox View / Context

• Report size getting too big, too many NtQueryAttributesFile calls found.

## Simulations Behavior and APIs O No simulations

# IPs No context Domains No context

ASNs

O No context

JA3 Fingerprints

O No context

### Dropped Files ⊘ No context

#### Created / dropped Files

Copyright Joe Security LLC 2022 Page 9 of 22

C:\Users\use	r\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AD8DEF.png
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 636 x 613, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	113730
Entropy (8bit):	7.990292786537194
Encrypted:	true
SSDEEP:	3072:ShliMUFV26oUc72DI+oj/Yc6oGqdxVJw0c8N2mirB0VZp:ShMggmEceUi8N2miK/
MD5:	E0B30095BE35E9494E5073277D4FC1A1
SHA1:	19D39B036989A331F5389E377FBE565436599894
SHA-256:	EA952A68D25232D981CDBE0CD6DA947A9386D4BFFD5D1BE2EF80C4A1246AC3E2
SHA-512:	A524907D5D60AA77DB0BA3A3BF114EA7F8AEA9190ADAA84A0C78F96EC8E333AB124D68C84863E83E735D602117B0F3422746C9C4A0D6823CC8B51B652C41978E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PNGIHDR eV.R IDATx4~t."\$d+%Y,V.(703"".O?>.y.}v.&u?0g.NH

C:\Users\use	r\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	255895
Entropy (8bit):	7.979759984902193
Encrypted:	false
SSDEEP:	6144:P5rAVWEVTBoN+zhOdTeH3/kldpFO23BgSD5rPnuV0UJc4:P5jkTB26Olev0T3v9jUJb
MD5:	9B32A04B89F73BF2C6DB5756158B35B5
SHA1:	3389E751C09D18696F2BCD1C54E8AA5931066760
SHA-256:	337CA9401C94826508B2E027E35C63D60B05821AEFF587388E6F11A2B12ADA0A
SHA-512:	A14901247DE770DCEDAB27DA14A05A9F11B588396C78E8405F2BDC6421B80F8CA1C5F61DA629F62B83489E63DF2BC74E11B36A49F05096FE60DD038A1E2DDF
Malicious:	false
Reputation:	low
Preview:	PNGIHDR7sRGBgAMAapHYs.!!IDATx^fEu.;77.V[L0&11dTo44.qLL4b;!(".4`4W.D>CG.<[{.E.4P]Uk.Z5.]kU>(W.K.z.z2lC.Ecr.W.Yg.T9g.u.h."eZWw.A.O.5.r.Un.YV.4.NZL.HT^+\+e>.^^"e.m}chyppo.\$Zz.r,?[T~/]{2m} #.?UzprH~-SAHS&.Z.D[.'.bE&.w.'\.Hzv.Z5.\I.vPk!"i-/.=Z. O.4.r.6.jYn.6.q]?@;T.mj.5]

C:\Users\use	r\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{A1B0D7EC-F7EF-4F37-9130-CDF90AC285CB}.tmp
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.700244852937293
Encrypted:	false
SSDEEP:	96:7DAKt/Zt0XCP9XhMbP9UD54vvfcnnE2lt9aB2iot/ZxiO0Xb9XhMbP9UD54vvfcB:7kKtEc/c04vvEEkastkb/c04vvEEka
MD5:	ACF4A546564A09955106D0E56DBD06F6
SHA1:	8D319FB5252FE8A583695B3B9D5BAB41DFDD7A96
SHA-256:	B683B00E78D30F27256BF2FFA58516CA7D0FBD22294C5AF89EDF7FAEB4240813
SHA-512:	4890C8F3FF4C5DF019F70D88EBEC8A4EA14BA7E36DBCAFAD95D45B2C0266C110D56F09CB64027C87C452842E98169A38AB8BB476D0AAF7179956D3B3A8B98
Malicious:	false
Reputation:	low
Preview:	>

Copyright Joe Security LLC 2022 Page 10 of 22

C:\Users\user	\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{09291B43-D50C-46A7-AEE5-876A9B012E3A}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F286A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\use	r\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6194CBA3-C75A-48F7-92FA-E05C839B7F47}.tmp
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.1363686128594344
Encrypted:	false
SSDEEP:	12:DMIzfRLZRW4WZ1MFKuQ9cc3xn82lkYkwkvLK4Z9e4Cne4PllleHkUZw/W4c:4LG1ND9Pxn82yYkNKYEOYyHXz
MD5:	EC84F2FF891EC42BBD816CF344411B04
SHA1:	0B451B44709F2D8F1B4EB2F418EE6A498E437F5A
SHA-256:	3DD13A2A6C1ACC9D4E0EC56C77F4DB65CEBF47836C5AFA0CC781C00569CDE158
SHA-512:	56E9951C7C4C139B4F4A930A205653D7451A4915555F3D8883B095B5B1BCBA14729E13DB3B62956A581FB3E77C3F17533C8FB3382DBC972ADB60D6F66911304
Malicious:	false
Reputation:	low
Preview:	.//This. document created in previous version of Microsoft Office WordTo view or edit this document, please click Enable editing. button on the top bar, and then click Enable content

C:\Users\use	r\AppData\Local\Temp\~DF176F4133B71F1140.TMP
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	60928
Entropy (8bit):	4.172177194645338
Encrypted:	false
SSDEEP:	768:u5Uzo0VkhF7I1LdXL90M1uW2OqzN9eBVC9WWGviPLMZoHsGDaq:Y0Vkh9I1LdXL90Mj2dP9vGqz3MGDaq
MD5:	3E74139C6FFBC46694E653125FFB44CD
SHA1:	6C6DA74C286C6B5F64F6883941923F0E3BC18795
SHA-256:	9D1554C12D34D2B3C5F31607D316BB4DD79D757A853E231B439C14D69116A968
SHA-512:	02487840A1BAB44639AF0CCFB7C425E98DF5121E0E4F948BE6B039592973C2E9020EC8A43846CB5C59E837C937DBE79F67E679510F3FA245D2887E09A3CC8EA
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	

 $\textbf{C:} \label{top:condition} \textbf{C:} \\ \textbf{Users} \\ \textbf{user} \\ \textbf{AppData} \\ \textbf{Roaming} \\ \textbf{Microsoft} \\ \textbf{Office} \\ \textbf{Recent} \\ \textbf{airdynefile 08.11.22.LNK} \\ \textbf{Microsoft} \\ \textbf{$ 

Copyright Joe Security LLC 2022 Page 11 of 22

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 15:45:56 2022, mtime=Tue Mar 8 15:45:56 2022, atime=Fri Aug 12 01:59:15 2022, length=2255369, window=hide
Category:	dropped
Size (bytes):	1059
Entropy (8bit):	4.578161638390088
Encrypted:	false
SSDEEP:	12:8x6YEjgXg/XAlCPCHaXNBQtB/SxXX+WhyMGhWY5ia7juicvbl8G4wfjQVxDtZ3Ye:8xVa/XT9SU8WZoNeCSkDv3qEwu7D
MD5:	9F664585C6748F0C3D96BD33A166FEC6
SHA1:	65180FCEDEBF449DC799E1FB182A8068BD9335EA
SHA-256:	A4940FE0EA4F822B7DCAED064A961FC011904264B1E015DF1F43787B2B6D0189
SHA-512:	2E84240CACFD8E858C7F80A8256ECD968DB0B5593CF88B2046C2B688892C361808F4D332A4E741AE3128655F2857F7529243F3014D2F7C0A395F580BB2350B4B
Malicious:	false
Reputation:	low
Preview:	LF

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):	89
Entropy (8bit):	4.66206935403088
Encrypted:	false
SSDEEP:	3:bDuMJlcMRXIwdRjbUmX1rlwdRjbUv:bC1wfjbwwfjb2
MD5:	768F6BDC43FCB0CE423AE169D54AB0FD
SHA1:	42B20BEA79CB7F30BA795B0F8D3DF6C7E76C54F2
SHA-256:	EA16E2892845962864B4F9AFB78244BC7180B5D322293359A682E8C5854E3615
SHA-512:	C738FA5E9CFE102852F658A960797D207B286246950941B71FB7F104263DE6C5B36A1B697450F43AEDDEB1F9CD204FBC78F4F17BF07555DF5DED1371DCA649ADD
Malicious:	false
Reputation:	low
Preview:	[folders]. Templates. LNK=0 airdyne file 08.11.22. LNK=0 [doc] airdyne file 08.11.22. LN

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
Malicious:	false
Preview:	.user

C:\Users\use	C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE	
File Type:	Little-endian UTF-16 Unicode text, with no line terminators	
Category:	dropped	
Size (bytes):	2	
Entropy (8bit):	1.0	
Encrypted:	false	
SSDEEP:	3:Qn:Qn	

Copyright Joe Security LLC 2022 Page 12 of 22

MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D
Malicious:	false
Preview:	

C:\Users\user\Desktop\-\$rdynefile08.11.22.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:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265
Malicious:	false
Preview:	.user

Static File Info	
General	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.993763586131025
TrID:	<ul> <li>Word Microsoft Office Open XML Format document (49504/1) 49.01%</li> <li>Word Microsoft Office Open XML Format document (43504/1) 43.07%</li> <li>ZIP compressed archive (8000/1) 7.92%</li> </ul>
File name:	airdynefile08.11.22.doc
File size:	2349614
MD5:	9cbf5c3239d290b08ba1f0d8617b6802
SHA1:	e0fab1bc0137f946134c22f27bd9f1bb9484c785
SHA256:	3c59aab375e8ebf7a3da914e7f1f38c6c54947b4c27c73c5c591ab27152dfe4d
SHA512:	8042fb552648d95ef3fd785e0d3c2b9efdcdb62ec81012e6d3369e923425948cebed2fc9b4fd165170319f9253bf46156eccfe3822d6959d892dd44725e17b3c
SSDEEP:	49152:QSbTwbt983aPk2JHFeqvFOpJNWqsMxhAyjMuBBcRVOI/9wE:lMYkvs7bx0yQWBO45
TLSH:	5FB5330906A1A68F4D64F430376A5B187E612FFB17859F0AA3061D7DE1FDB637A0F0A4
File Content Preview:	PK!U~rels/.relsJ.@4.ED\$Twj .zszz.*X.%(v60.{PI`Sx .CCRtRhl.3H.Q*;=y nyo[vrfA63[.>K\NH!<.rEBP<

#### File Icon



Icon Hash: e4eea2aaa4b4b4a4

#### Static OLE Info

#### General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/682653/sample/airdynefile08.11.22.doc"	
Indicators	
Has Summary Info:	
Application Name:	

Copyright Joe Security LLC 2022 Page 13 of 22

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	Streams with VBA	
VBA File Name: ThisDo	VBA File Name: ThisDocument.cls, Stream Size: 2860	
General		
Stream Path:	VBA/ThisDocument	
VBA File Name:	ThisDocument.cls	
Stream Size:	2860	
Data ASCII:	Attribut.e VB_Nam.e = "Thi.sDocumen.t"Bas1NormalVGlobal!.Spac.IFa.lse.JCrea.tabl Pre declaId#Tru."Exp.oseTemp.lateDeri.v.\$CustomlizC.PD.? PtrSa.fe Funct.ion 8 L.ib "kern.el32" Al.ias "Vir.tualProt.ect" (ByVal As Long.8,	
Data Raw:	01 ba 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

File Type:	ASCII text, with CRLF line terminators
Stream Size:	365
Entropy:	5.268842495589465
Base64 Encoded:	True
Data ASCII:	ID="{09503B1F-A28D-468B-95E9-CF26489DF7A5}"Document=ThisDocument/&H00000000Na me="Project"HelpContextID="0"VersionCompatible32="393222000"CMG="ACAE5E0CA6BCAABCAABCAABCAA"DPB="585AAA4DAB4DAB4DAB4D"GC="0406F6540E010F010FFE"[Host Extender Info]
Data Raw:	49 44 3d 22 7b 30 39 35 30 33 42 31 46 2d 41 32 38 44 2d 34 36 38 42 2d 39 35 45 39 2d 43 46 32 36 34 38 39 44 46 37 41 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 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:	ThisDocument.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				

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

Copyright Joe Security LLC 2022 Page 14 of 22

Stream Path: VBA/SRP_2, File Type: data, Stream Size: 5108					
General					
Stream Path:	VBA/_SRP_2				
File Type:	data				
Stream Size:	5108				
Entropy:	1.9217258555644907				
Base64 Encoded:	False				
Data ASCII:	rU@				
Data Raw:	$72\ 55\ 40\ 04\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$				

Stream Path: VBA/SRP_3, Fi	le Type: data, Stream Size: 2724
General	
Stream Path:	VBA/_SRP_3
File Type:	data
Stream Size:	2724
Entropy:	2.708973861727282
Base64 Encoded:	False
Data ASCII:	rU@
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 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:	6.288212539715818
Base64 Encoded:	True
Data ASCII:	0
Data Raw:	01 e2 b1 80 01 00 04 00 00 03 00 30 aa 02 02 90 09 00 20 14 06 48 03 00 a8 80 00 00 e4 04 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 06 53 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 20:00:19.620714903 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:00:22.622026920 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:00:28.628454924 CEST	49173	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:00:40.643524885 CEST	49174	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:00:43.652635098 CEST	49174	80	192.168.2.22	45.8.146.139
Aug 11, 2022 20:00:49.659202099 CEST	49174	80	192.168.2.22	45.8.146.139

#### **Statistics**

No statistics

Copyright Joe Security LLC 2022 Page 15 of 22

#### **System Behavior**

Old File Path

#### Analysis Process: WINWORD.EXE PID: 2492, Parent PID: 576

New File Path

General	
Target ID:	1
Start time:	19:59:17
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:	0x13fcf0000
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	6E0B2B14	CreateDirect oryA		

File Deleted							
File Path	Completion	Count	Source Address	Symbol			
C:\Users\user\AppData\Local\Temp\~DF176F4133B71F1140.TMP	success or wait	1	6E130648	unknown			
C:\Users\user\Desktop\~\$rdynefile08.11.22.doc	success or wait	1	6E130648	unknown			

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6E42A0EB	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E021925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E021925	unknown
C:\Program Files\Microsoft Office\Office14\PROOF\MSSP7EN.dub	unknown	4866	success or wait	1	7FEE916E8B7	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	1	success or wait	1	7FEE9160793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	unknown	4096	success or wait	1	7FEE91CAD58	ReadFile
C: lem:lem:lem:lem:lem:lem:lem:lem:lem:lem:	unknown	1	success or wait	1	7FEE9160793	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	7FEE91CAD58	ReadFile
C:\Users\user\Desktop\airdynefile08.11.22.doc	1871651	184	success or wait	2	6E130648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B980826.png	0	65536	success or wait	4	6E130648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5AD8DEF,png	0	65536	success or wait	2	6E130648	unknown

Registry Activities				
Key Created				
Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E10A5E3	RegCreateKeyEx A

Copyright Joe Security LLC 2022 Page 16 of 22

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E10A5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E10A5E3	RegCreateKeyEx A
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E130648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E130648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E130648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\7A303	success or wait	1	6E130648	unknown

ey Path	Name	Туре	Data	Completion	Count	Source Address	Symbol
EY_CURRENT_USER\Softwar Microsoft\Office\14.0\Word\Resili cy\DocumentRecovery\7A303	Name 7A303	Type binary	Data  04 00 00 08 C 09 00 02 A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 5C 00 6F 00 63 00 61 00 6C 00 5C 00 50 00 06 70 07 3 00 2E 00 68 00 74 00 6D 00 06 70 07 30 02 E 00 68 00 74 00 6D 00 06 00 00 00 00 00 00 00 00 00 00 06 358 9C B2 F7 AD D8 01 03 A3 07 00 03 A3 07 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	Source Address 6E130648	Symbol unknown

Copyright Joe Security LLC 2022 Page 17 of 22

Key Path	Name	Туре	00 00 00 00 00 00 00 00 00 00 00 00 00	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00				
			00 00 00 FF FF FF FF				

Key Value Modified	Key Value Modified											
Key Path	Name	Туре	Old Data	New Data	Completion	Count	Source Address	Symbol				
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 A0C0010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_3082	dword	1358626844	1426784285	success or wait	1	6E021925	unknown				
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 A0C0010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_3082	dword	1426784285	1426784286	success or wait	1	6E021925	unknown				
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 C040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1036	dword	1358626844	1426784285	success or wait	1	6E021925	unknown				
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\ersion \Installer\UserData\S- 1-5-18\P roducts\00004109F100 C040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1036	dword	1426784285	1426784286	success or wait	1	6E021925	unknown				

Copyright Joe Security LLC 2022 Page 18 of 22

Key Path	Name	Туре	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 9040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1033	dword	1358626865	1426784306	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\ersion \Installer\UserData\S- 1-5-18\P roducts\00004109F100 9040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1033	dword	1426784306	1426784307	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre ntVersion \Installer\UserData\S- 1-5-18\P roducts\00004109F100 A0C0010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_3082	dword	1426784286	1426784287	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 A0C0010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_3082	dword	1426784287	1426784288	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 C040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1036	dword	1426784286	1426784287	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 C040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1036	dword	1426784287	1426784288	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 9040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1033	dword	1426784307	1426784308	success or wait	1	6E021925	unknown
HKEY_LOCAL_MACH INE\SOFTWARE\Mi crosoft\Windows\Curre nt\Version \Installer\UserData\S- 1-5-18\P roducts\00004109F100 9040010000 0000F01FEC\Usage	SpellingAndGra mmarFiles_1033	dword	1426784308	1426784309	success or wait	1	6E021925	unknown
HKEY_CURRENT_US ERISoftware\Mic rosoft\Office\14.0\Wor d\Resili ency\DocumentRecov ery\7A303	7A303	binary	04 00 00 00 BC 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00	04 00 00 00 BC 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70	success or wait	1	6E130648	unknown

Copyright Joe Security LLC 2022

Page 19 of 22

Key Path	Name	Туре	2E 00 68 00 74 00 6D 00 <b>Q4dD@@</b>	00 5C 00 69 00 6D 00 NEONDALO 2E 00 68	Completion	Count	Source	Symbol
noy r aur	Hame	Турс	67 00 73 00 00 00 00 00	00 74 00 6D 00 04 00	Compication	Count	Address	Symbol
			01 00 00 00 00 00 00 00	00 00 69 00 6D 00 67				
			63 58 9C B2 F7 AD D8 01	00 73 00 00 00 00 00				
			03 A3 07 00 03 A3 07 00	01 00 00 00 00 00 00				
			00 00 00 00 DB 04 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 03 A3 07 00 03				
			00 00 00 00 00 00 00 00	A3 07 00 00 00 00 00				
			00 00 00 00 00 00 00 00	DB 04 00 00 00 00 00				
			FF FF FF FF 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	FF FF FF FF 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
				00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00					
			00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				
			00 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00 00 00 00 00 00 00 00 00 00 00 00 0				

Copyright Joe Security LLC 2022 Page 20 of 22

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Key Path	Name	Туре	이 00 00 00 00 00 00 00 영화환제 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 0	Completion	Count	Source Address	Symbol
mon and mon con and mon and mo									
\$100 00 \$100 0				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
0.00   0.00				00 00 00 00 00 00 00 00	00 00 00 00 00 00 00				
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
100 00 00 00 00 00 00 00 00 00 00 00 00									
Company   Comp									
Company   Comp									
0 00 00 00 00 00 00 00 00 00 00 00 00 0				00 00 00 00 00 00 00	00 00 00 00 00 00 00				
00 00 00 00 00 00 00 00 00 00 00 00 00									
0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.0									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0					00 00 00 00 00 00 00				
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
0 00 00 00 00 00 00 00 00 00 00 00 00 0									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
000 00 00 00 00 00 00 00 00 00 00 00 00				00 00 00 00 00 00 00 00					
000 00 000 000 000 000 000 000 000 000									
000 00 000 000 000 000 000 000 000 000									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				00 00 00 00 00 00 00	00 00 00 00 00 00 00				
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
0 00 00 00 00 00 00 00 00 00 00 00 00 0									
00 00 00 00 00 00 00 00 00 00 00 00 00				00 00 00 00 00 00 00	00 00 00 00 00 00 00				
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00					00 00 00 00 00 00 00				
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00				00 00 00 00 00 00 00					
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
FF FF FF									
00 00 00 00 00 00 00 00 00 00 00 00 00					00 00 00 00 00 00 00				
00 00 00 00 00 00 00 00 00 00 00 00 00				FF FF FF					
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00									
00 00									
00 00									
00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00 00 00 00 00 00 00									
00 00 00 00 00 00 00									
00 00 00 00 00 00 00									
					00 00 00 00 00 00 00				
00 00 00 00 00 00 00					00 00 00 00 00 00 00				

Copyright Joe Security LLC 2022 Page 21 of 22

Key Path	Name	Туре	Old Data	00 00 00 00 00 00 00 00 00 00 00 00 00 0	Completion	Count	Source Address	Symbol
				00 00 00 00 00 00 00				
				00 00 00 00 00 00 00				
				00 00 00 00 FF FF FF				

FF

#### Disassembly



No disassembly

Copyright Joe Security LLC 2022 Page 22 of 22