ID: 332012
Sample Name: COVID-Trial-Application-Frm09874x.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 23:47:16
Date: 17/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

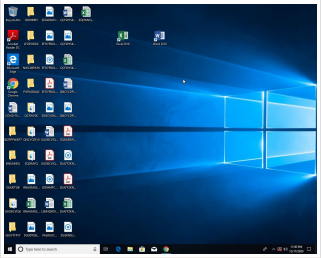
Analysis Report COVID-Trial-Application-Frm09874x.docx

Overview

General Information

Sample Name:	COVID-Trial-Application-Frm09874x.docx
Analysis ID:	332012
MD5:	0343741d7f9a129.
SHA1:	5aae176e9f1b983.
SHA256:	61e5c441089b95..

Most interesting Screenshot:



Errors

⚠ Corrupt sample or wrongly selected analyzer.

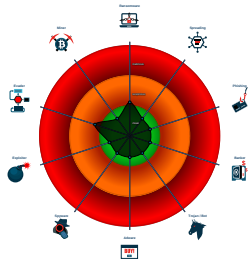
Detection

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 5532 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

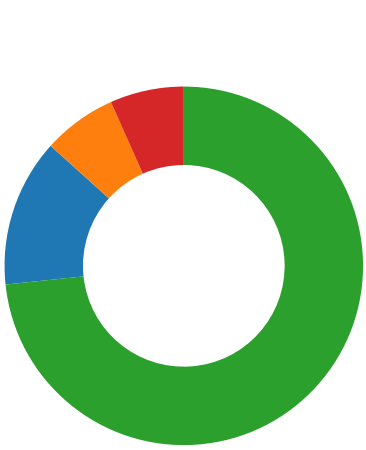
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

AV Detection:

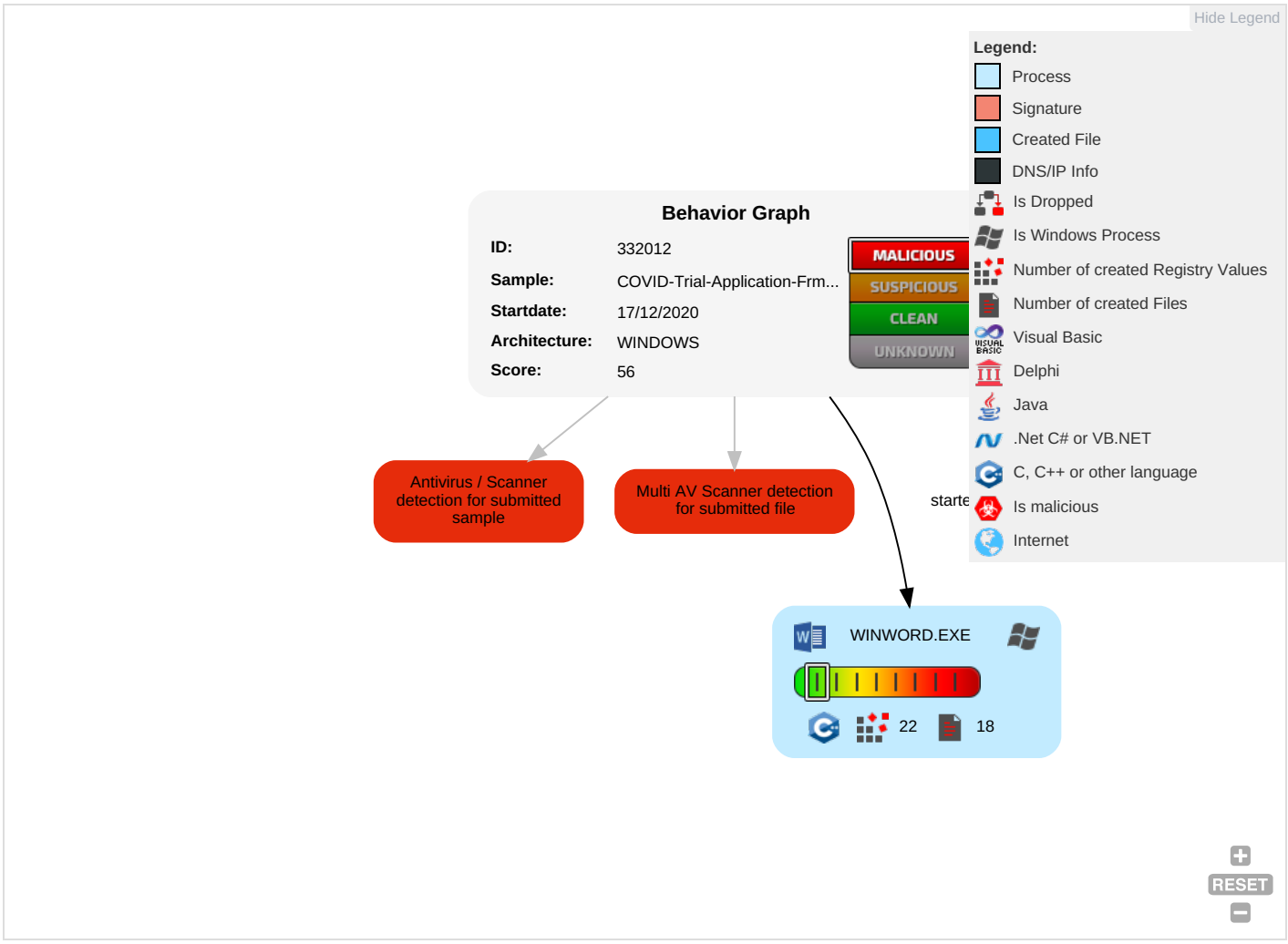
Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

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	Scripting 2	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

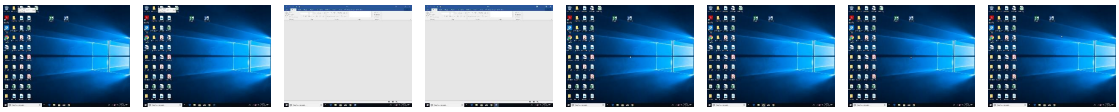
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
COVID-Trial-Application-Frm09874x.docx	72%	Virustotal		Browse
COVID-Trial-Application-Frm09874x.docx	58%	Metadefender		Browse
COVID-Trial-Application-Frm09874x.docx	79%	ReversingLabs	Document-Word.Trojan.Powload	
COVID-Trial-Application-Frm09874x.docx	100%	Avira	W97M/Agent.2646611	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://login.microsoftonline.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://shell.suite.office.com:1443	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://autodiscover-s.outlook.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://cdn.entity.	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://wus2-000.contentsync.	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://powerlift.acompli.net	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://cortana.ai	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://api.aadrm.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://api.microsoftstream.com/api/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://cr.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://graph.ppe.windows.net	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://store.office.cn/addinstemplate	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://globaldisco.crm.dynamics.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://web.microsoftstream.com/video/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://graph.windows.net	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://dataservice.o365filtering.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://weather.service.msn.com/data.aspx	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://apis.live.net/v5.0/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://management.azure.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://incidents.diagnostics.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://entitlement.diagnostics.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://outlook.office.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://templatelogging.office.com/client/log	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://outlook.office365.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://webshell.suite.office.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://management.azure.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://ncus-000.contentsync.	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://devnull.onenote.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://messaging.office.com/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeenti ties	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://augloop.office.com/v2	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://skyapi.live.net/Activity/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://dataservice.o365filtering.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	2BFC9729-7240-42A6-948B-B179BBA29E7A.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	332012
Start date:	17.12.2020
Start time:	23:47:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-Trial-Application-Frm09874x.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.winDOCX@1/3@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.64.90.137, 52.109.76.68, 52.109.8.22, 52.109.88.39, 51.11.168.160, 92.122.144.200, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.104.139.180 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, europe.configsvc1.live.com.akadns.net
Errors:	• Corrupt sample or wrongly selected analyzer.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2BFC9729-7240-42A6-948B-B179BBA29E7A	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2BFC9729-7240-42A6-948B-B179BBA29E7A	
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	130397
Entropy (8bit):	5.377002666775828
Encrypted:	false
SSDEEP:	1536:pcQceNgrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:0mQ9DQW+zBX8P
MD5:	54F78A83E2198C918D819C95AA40DDEF
SHA1:	6BDCEB62245E03A4A96CF6E4CD077B51CBF96F66
SHA-256:	CE4BF4AA5119F15A99188972A4F71B684A72F9F105528DD50C40CA9DCB15801A
SHA-512:	1B72C780A97FC6F94136A5D5721D08F31B4B7CEA2C740B9B34E49B0BCCE3674596F29F7B61ABE6560B1F08223C459757A7B06CB6BEB51F94B01CD3F11F3C09BE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-12-17T22:48:04">.. Build: 16.0.13616.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9173A544-D419-425B-8320-EF84077A8E0E}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.65546677858913
Encrypted:	false
SSDEEP:	3:Rl/ZdasSxlqbi+t/tlqfg+ERtl7:RtZzHbdtSf7yt5
MD5:	DC1D66230F7BA2A7AF582C8E5C2F61FD
SHA1:	3B04CB05BEB39EBFE97C718E3981D6D4CC72CBBB
SHA-256:	78F4DF62D1ABF1B05837BF92505079F803AC218D89B3ADF495F362C8153AFF7A
SHA-512:	7DCBC139C02DAF2C4608DA2DEC1B5DFB2BCF8CB71E57EA359ACC93C51C3ACD968D587FF0D3FF515701CC4DBBB190079754F43D22AC2405B372895BA6C7AC4D3
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....@...y[.A.7.....$.....6C..E.8.}[.A38.....T.....6C..A.F..[.AA9.....$...

Static File Info

General

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Neque., Author: Emilie Mercier, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Aug 26 07:08:00 2020, Last Saved Time/Date: Wed Aug 26 07:08:00 2020, Number of Pages: 1, Number of Words: 3, Number of Characters: 20, Security: 0
Entropy (8bit):	6.692763082766669
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	COVID-Trial-Application-Frm09874x.docx
File size:	225324
MD5:	0343741d7f9a129e1c3af74963343140
SHA1:	5aae176e9f1b9830a498e549aa329b253f40a57f
SHA256:	61e5c441089b95c7879100b308aff42f8e7a059a4f3a5bc861ebd4d25fef58fc
SHA512:	d8088877776f75057d42ab8e03b4c606bf83d7c77cd6cec7b6d641fde97ae9a756dc1a3f2e4a45d5f88bdeadd63c2c045b9a571dd6942b951841615bd5fd3a7a
SSDEEP:	3072:dYy0u8YGgjv+ZvchmkHcl/o1/Vb6////////////////////////2:30uXnWFchmmcl/o1/2zcLwWSeCC
File Content Preview:	.....>.....{.....1...2...4...|..... .....

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "COVID-Trial-Application-Frm09874x.docx"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
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:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252
Title:	Neque.
Subject:	
Author:	Emilie Mercier
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	
Revion Number:	1
Total Edit Time:	0
Create Time:	2020-08-26 06:08:00
Last Saved Time:	2020-08-26 06:08:00

Summary	
Number of Pages:	1
Number of Words:	3
Number of Characters:	20
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Document Code Page:	1252
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: Her87_tsa69n, Stream Size: -1

General	
Stream Path:	Macros/Her87_tsa69n
VBA File Name:	Her87_tsa69n
Stream Size:	-1
Data ASCII:	
Data Raw:	

VBA Code Keywords

Keyword
Resume
CSng(dKkk))
False
"ds[]a")
VB_Base
"Lnwjsi_gqorknjswkz
VB_Creatable
VB_Exposed
VB_TemplateDerived
Error
Attribute
VB_PredeclaredId
VB_GlobalNameSpace
VB_Name
showwindow
Function
VB_Customizable

VBA Code

VBA File Name: Her87_tsa69n, Stream Size: 14642

General	
Stream Path:	Macros/VBA/Her87_tsa69n
VBA File Name:	Her87_tsa69n
Stream Size:	14642
Data ASCII:	. . . . L . . . . ' . . . . * . . . . N . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 20 05 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 27 05 00 00 af 2a 00 00 00 00 00 00 01 00 00 00 0a 93 1f 4e 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 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

VBA Code Keywords

Keyword
Resume
CSng(dKkk))
False
"ds[]a")
VB_Base
"Lnwjsi_gqorknjswkz
VB_Creatable
VB_Exposed
VB_TemplateDerived
Error
Attribute
VB_PredeclaredId
VB_GlobalNameSpace
VB_Name
showwindow
Function
VB_Customizable

VBA Code

VBA File Name: Y1cfhtdfo8an, Stream Size: 1333

General	
Stream Path:	Macros/VBA/Y1cfhtdfo8an
VBA File Name:	Y1cfhtdfo8an
Stream Size:	1333
Data ASCII:	. . . . V . . . . > . . . . { . . . . < . . . . . J . . . . : Y G . 8 , ... / . , . . . X D . .] . . ` . . . . @ . . . $. S . . . . x . . . . @ . . . $. S . . J . . . . : Y G . 8 , ... M E . . . .
Data Raw:	01 16 01 00 06 00 01 00 00 56 03 00 00 e4 00 00 00 ea 01 00 00 84 03 00 00 92 03 00 00 3e 04 00 00 01 00 00 00 01 00 00 00 0a 93 7b c4 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 3c 00 ff ff 00 00 4a f8 80 db 0e 3a 59 47 b7 38 2c f7 e2 11 cc 1f 2f d3 2c 81 f8 05 58 44 bf a2 5d ee f0 60 cf f6 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
Private
VB_Exposed
Attribute
VB_Creatable
VB_Name
Document_open()
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 114

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	114
Entropy:	4.2359563651

General	
Base64 Encoded:	True
Data ASCII:	. . . . F . . . M i c r o s o f t W o r d 9 7 - 2 0 0 3 D o c u m e n t . . . . . M S W o r d D o c . . . . . W o r d . D o c u m e n t . 8 . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 06 09 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 57 6f 72 64 20 39 37 2d 32 30 30 33 20 44 6f 63 75 6d 65 6e 74 00 0a 00 00 00 4d 53 57 6f 72 64 44 6f 63 00 10 00 00 00 57 6f 72 64 2e 44 6f 63 75 6d 65 6e 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 352

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	352
Entropy:	2.611686106
Base64 Encoded:	False
Data ASCII:	. . . . + , . . D . . . . + , . . , ... h . . . . p . . . . | . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 44 00 00 00 05 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 2c 01 00 00 e8 00 00 00 0c 00 00 00 01 00 00 00 68 00 00 00 0f 00 00 00 70 00 00 00 05 00 00 00 7c 00 00 00 06 00 00 00 84 00 00 00 11 00 00 00 8c 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 420

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	420
Entropy:	3.2280454647
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . t . . . . d . . . . L . . . . , ... 4 . . . . < . . . . D . . . . N o r m a l . d o t m .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 74 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 64 01 00 00 03 00 00 00 98 00 00 00 04 00 00 00 4c 01 00 00 05 00 00 00 a4 00 00 00 06 00 00 00 b0 00 00 00 07 00 00 00 bc 00 00 00 08 00 00 00 d0 00 00 00 09 00 00 00 dc 00 00 00

Stream Path: 1Table, File Type: data, Stream Size: 7035

General	
Stream Path:	1Table
File Type:	data
Stream Size:	7035
Entropy:	5.99786922232
Base64 Encoded:	True
Data ASCII:	. . . . s . . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . .
Data Raw:	06 06 0f 00 12 00 01 00 73 01 0f 00 07 00 03 00 00 00 03 00 00 00 04 00 08 00 00 00 98 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 9e 00 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 36 06 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 136573

General	
Stream Path:	Data
File Type:	data
Stream Size:	136573
Entropy:	7.24646975637
Base64 Encoded:	True
Data ASCII:	} . . . D . d . . . . G 3 . . . . p . . . . A . . . . ? . . . . y . 4 . l . 8 . a . m . 5 . u . h . . . P . i . c . t . u . r . e . . 1 . . . T . y . 4 . l . 8 . a . m . 5 . u . h . . . . . " . . . . R . . . . + i . . . ` . .

General	
Data Raw:	7d 15 02 00 44 00 64 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 bf 47 33 1f fe 01 fe 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0f 00 04 f0 a2 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 83 00 0b f0 70 00 00 00 04 41 01 00 00 00 05 c1 16 00 00 00 3f 01 00 00 06 00 bf 01 00 00 10 00 ff 01 00 00

Stream Path: Macros/Her87_tsa69n/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	Macros/Her87_tsa69n/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 296

General	
Stream Path:	Macros/Her87_tsa69n/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	296
Entropy:	4.62977558511
Base64 Encoded:	True
Data ASCII:	VERSION 5.00 . . Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} Her87_tsa69n . . Caption = "UserForm1". . ClientHeight = 3015 . . ClientLeft = 120 . . ClientTop = 465 . . ClientWidth = 4560 . . StartUpPosition = 1 'Cente
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 48 65 72 38 37 5f 74 73 61 36 39 6e 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20

Stream Path: Macros/Her87_tsa69n/f, File Type: data, Stream Size: 506

General	
Stream Path:	Macros/Her87_tsa69n/f
File Type:	data
Stream Size:	506
Entropy:	4.02860334569
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . . 0 . . . . . P . . . . . jdr84jj64f1s45_bs . . . . . , ... L . . . . . Sdavaseq_ztmb1pm . . . . . 0 . . . . . @ . . . . . Ihu_f5_wgnmr78o_xy . . . . . .(. . . . . L . . . . . Rfno8gmlf5un . . . . . 8 . . . . .
Data Raw:	00 04 20 00 08 0c 00 0c 09 00 00 00 12 00 00 00 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 cc 01 00 00 00 89 01 00 00 00 30 00 e5 01 00 00 12 00 00 80 01 00 00 00 50 00 00 00 00 00 19 00 5a 6a 64 72 38 34 6a 6a 36 34 66 31 73 34 35 5f 62 73 00 00 00 00 00 00 00 00 00 00 00 00 2c 00 e5 01 00 00 0e 00 00 80 02 00 00 00 4c 00 00 00 01 00 19 00 53 64

Stream Path: Macros/Her87_tsa69n/i05/\x1CompObj, File Type: data, Stream Size: 112

General	
Stream Path:	Macros/Her87_tsa69n/i05/\x1CompObj
File Type:	data
Stream Size:	112
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . . .n` . . . . . `. . . . . Microsoft Forms 2.0 Frame . . . . . Embedded Object . . . . . Forms.Frame.1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i05/f, File Type: data, Stream Size: 44

General	
Stream Path:	Macros/Her87_tsa69n/i05/f
File Type:	data
Stream Size:	44
Entropy:	2.0683698489
Base64 Encoded:	False
Data ASCII:	. . . @ . . . . . } . . . . .
Data Raw:	00 04 20 00 40 0c 02 08 04 80 00 00 03 00 00 00 00 7d 00 00 c4 1d 00 00 d8 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i05/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/Her87_tsa69n/i05/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/Her87_tsa69n/i07/\x1CompObj, File Type: data, Stream Size: 112

General	
Stream Path:	Macros/Her87_tsa69n/i07/\x1CompObj
File Type:	data
Stream Size:	112
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . n ` . . . . . ` . . . . . M i c r o s o f t F o r m s 2 . 0 F r a m e . . . . . E m b e d d e d O b j e c t . . . . . F o r m s . F r a m e . 1 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i07/f, File Type: data, Stream Size: 44

General	
Stream Path:	Macros/Her87_tsa69n/i07/f
File Type:	data
Stream Size:	44
Entropy:	2.0683698489
Base64 Encoded:	False
Data ASCII:	. . . @ . . . . . } . . . . .
Data Raw:	00 04 20 00 40 0c 02 08 04 80 00 00 03 00 00 00 00 7d 00 00 c4 1d 00 00 d8 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: Macros/Her87_tsa69n/i07/o, File Type: empty, Stream Size: 0

General	
Stream Path:	Macros/Her87_tsa69n/i07/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: Macros/Her87_tsa69n/o, File Type: data, Stream Size: 24080

General	
Stream Path:	Macros/Her87_tsa69n/o
File Type:	data
Stream Size:	24080
Entropy:	4.52861483723
Base64 Encoded:	True

General	
Data ASCII:	. . 0 . A . E . . . . . . H . , ... { . . . U g z w t m i u _ g d d 1 z g w 5 I . . . . . . 5 . . . . T a h o m a . . . . , . A . E . . . . . . H . , ... { . . . U t 5 k y u f z j j c 3 1 q a m . . . . 5 . . . . T a h o m a . . . . . A . E . . . . . . H . , ... { . . . P . . . . . . 5 . . . . T a h o m a 6 . . . , . A . E . . . . . . H . , ... { . . . T l 0 2
Data Raw:	00 02 30 00 41 01 45 80 00 00 00 00 1b 48 80 2c 03 01 02 00 11 00 00 80 ec 09 00 00 7b 02 00 00 55 67 7a 77 74 6d 69 75 5f 67 64 64 31 7a 67 77 35 49 2e 0f 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00 00 02 00 00 54 61 68 6f 6d 61 00 00 00 02 2c 00 41 01 45 80 00 00 00 00 1b 48 80 2c 03 01 02 00 10 00 00 80 ec 09 00 00 7b 02 00 00 55 74 35 6b 79 75 66 7a 6a 6a 63 33 31 71 61 6d

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 510

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	510
Entropy:	5.41307394677
Base64 Encoded:	True
Data ASCII:	I D = " { 0 3 7 6 D 7 E 2 - 8 1 E 5 - 4 D 0 2 - A 8 E 9 - 3 E 2 0 E A 5 A 7 2 C 4 } " . . D o c u m e n t = Y 1 c f h t d f o 8 a n / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = H e r 8 7 _ t s a 6 9 n . . E x e N a m e 3 2 = " J t j c n g c 1 j 8 c j 7 x q s e " . . 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 = " 7
Data Raw:	49 44 3d 22 7b 30 33 37 36 44 37 45 32 2d 38 31 45 35 2d 34 44 30 32 2d 41 38 45 39 2d 33 45 32 30 45 41 35 41 37 32 43 34 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 59 31 63 66 68 74 64 66 6f 38 61 6e 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 80

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	80
Entropy:	3.47192809489
Base64 Encoded:	False
Data ASCII:	Y 1 c f h t d f o 8 a n . Y . 1 . c . f . h . t . d . f . o . 8 . a . n . . . H e r 8 7 _ t s a 6 9 n . H . e . r . 8 . 7 . _ . t . s . a . 6 . 9 . n . . . . .
Data Raw:	59 31 63 66 68 74 64 66 6f 38 61 6e 00 59 00 31 00 63 00 66 00 68 00 74 00 64 00 66 00 6f 00 38 00 61 00 6e 00 00 00 48 65 72 38 37 5f 74 73 61 36 39 6e 00 48 00 65 00 72 00 38 00 37 00 5f 00 74 00 73 00 61 00 36 00 39 00 6e 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 14330

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	14330
Entropy:	5.40893568443
Base64 Encoded:	True
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 2 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/__SRP_0, File Type: data, Stream Size: 1534

General	
Stream Path:	Macros/VBA/__SRP_0
File Type:	data
Stream Size:	1534
Entropy:	4.52531312411
Base64 Encoded:	False
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ h . . . . 1 . . . . v . . E E . z . . . S . 9 . . . . e . . . . y . . . . Q . . . .

General	
Data Raw:	93 4b 2a a3 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00

Stream Path: Macros/VBA/__SRP_1, File Type: data, Stream Size: 106

General	
Stream Path:	Macros/VBA/__SRP_1
File Type:	data
Stream Size:	106
Entropy:	2.10825159249
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ } . . . . . p . . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 7d 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 ff ff ff ff 03 00 00 09 11 03 00 00 00 00 00 00 09 08 00 00 00 00 00 00 08 00 00 00 00 00 01 00 70 00 00 7f 00 00 00 00

Stream Path: Macros/VBA/__SRP_2, File Type: data, Stream Size: 304

General	
Stream Path:	Macros/VBA/__SRP_2
File Type:	data
Stream Size:	304
Entropy:	2.29666421023
Base64 Encoded:	False
Data ASCII:	r U . . . . . 0 . . . . . i . . . . . 4 . . . . . a . . . . . 1 . . . . . ` . . . . . 0 . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 01 00 01 00 00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 b9 07 00 00 00 00 00 00 e1 07 00 00 00 00 00 00 09 00 00 00 01 00 02 00 69 07 00 00 00 00 00 00 08 00 0d 00 34 00 00 00 09 08 00 00 00 00 00 00 61 00 00 00 00 00

Stream Path: Macros/VBA/__SRP_3, File Type: data, Stream Size: 103

General	
Stream Path:	Macros/VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	2.16020154321
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . $ . . . . . ` . . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 40 00 00 00 04 00 24 00 01 01 00 00 00 00 02 00 00 00 04 60 00 00 ec 06 1c 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: Macros/VBA/dir, File Type: MIPSEB MIPS-III ECOFF executable not stripped - version 72.3, Stream Size: 836

General	
Stream Path:	Macros/VBA/dir
File Type:	MIPSEB MIPS-III ECOFF executable not stripped - version 72.3
Stream Size:	836
Entropy:	6.4798951851
Base64 Encoded:	True
Data ASCII:	. @ . . . . . 0 * . . . . . p . . H . . . . . d . . . . . N o r m a l r r Q . (. . @ . . . . . = ... l . . . . . y 7 3 a . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \ \ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \ \ W i n d o w s . \ \ S y s W O W 6 4 \ \ . 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 Q . F . . . . . * , \ \ C . . . . V . m . .
Data Raw:	01 40 b3 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 4e 6f 72 6d 61 6c 72 72 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 79 37 33 61 0d 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Stream Path: WordDocument, File Type: data, Stream Size: 4096

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.23871150966
Base64 Encoded:	False
Data ASCII:	. . . . [. . . . . b j b j . . . . . p a ! \\ p ! \\ . . . . . s . . . . . s . . . . . s . . . . . s . . . . . s . . . . .
Data Raw:	ec a5 c1 00 5b e0 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 17 08 00 00 0e 00 62 6a 62 6a 12 0b 12 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 70 61 21 5c 70 61 21 5c 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 0f 00 00 00 00 00 00 00 00 00 ff ff 0f 00 00 00 00 00

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 17, 2020 23:47:58.559408903 CET	60100	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:47:58.586616039 CET	53	60100	8.8.8.8	192.168.2.3
Dec 17, 2020 23:47:59.234249115 CET	53195	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:47:59.269339085 CET	53	53195	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:00.256105900 CET	50141	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:00.280672073 CET	53	50141	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:01.414206982 CET	53023	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:01.449753046 CET	53	53023	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:02.798089027 CET	49563	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:02.825485945 CET	53	49563	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:04.010288000 CET	51352	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:04.043447971 CET	53	51352	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:04.717091084 CET	59349	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:04.752000093 CET	53	59349	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:05.204874992 CET	57084	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:05.241971970 CET	53	57084	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:05.381069899 CET	58823	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:05.405482054 CET	53	58823	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:06.200277090 CET	57084	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:06.237274885 CET	53	57084	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:06.415813923 CET	57568	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:06.443052053 CET	53	57568	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:07.217051983 CET	57084	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:07.252794027 CET	53	57084	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:07.460062027 CET	50540	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:07.484452963 CET	53	50540	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:08.497672081 CET	54366	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:08.524774075 CET	53	54366	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:09.150320053 CET	53034	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:09.231875896 CET	57084	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:09.247699976 CET	53	53034	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:09.264218092 CET	53	57084	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:13.232331991 CET	57084	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:13.268145084 CET	53	57084	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:25.118901014 CET	57762	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:25.146229029 CET	53	57762	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:33.074155092 CET	55435	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:33.108650923 CET	53	55435	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:38.205765963 CET	50713	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:38.246542931 CET	53	50713	8.8.8.8	192.168.2.3
Dec 17, 2020 23:48:59.364485025 CET	56132	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:48:59.391777039 CET	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 17, 2020 23:49:02.318661928 CET	58987	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:49:02.354931116 CET	53	58987	8.8.8.8	192.168.2.3
Dec 17, 2020 23:49:33.798738956 CET	56579	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:49:33.825829983 CET	53	56579	8.8.8.8	192.168.2.3
Dec 17, 2020 23:49:35.324107885 CET	60633	53	192.168.2.3	8.8.8.8
Dec 17, 2020 23:49:35.364978075 CET	53	60633	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5532 Parent PID: 792

General

Start time:	23:48:03
Start date:	17/12/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x11e0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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 Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly