ID: 319766
Sample Name:
1118_8732615.doc
Cookbook: default.jbs
Time: 16:22:59
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

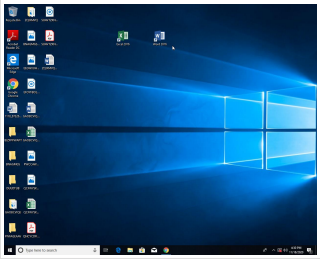
Analysis Report 1118_8732615.doc

Overview

General Information

Sample Name:	1118_8732615.doc
Analysis ID:	319766
MD5:	0f75ad40daec01a.
SHA1:	76334ccc6e92d5...
SHA256:	afba9deb16b5100.
Tags:	doc Hancitor macros

Most interesting Screenshot:



Errors

⚠ Corrupt sample or wrongly selected analyzer.

Detection

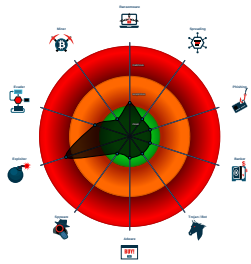
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Machine Learning detection for samp…
- Yara detected hidden Macro 4.0 in E…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 2440 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

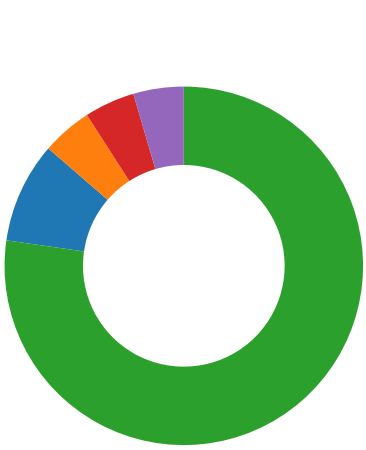
Initial Sample

Source	Rule	Description	Author	Strings
1118_8732615.doc	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Document contains an embedded VBA macro which may execute processes

Document contains an embedded VBA macro with suspicious strings

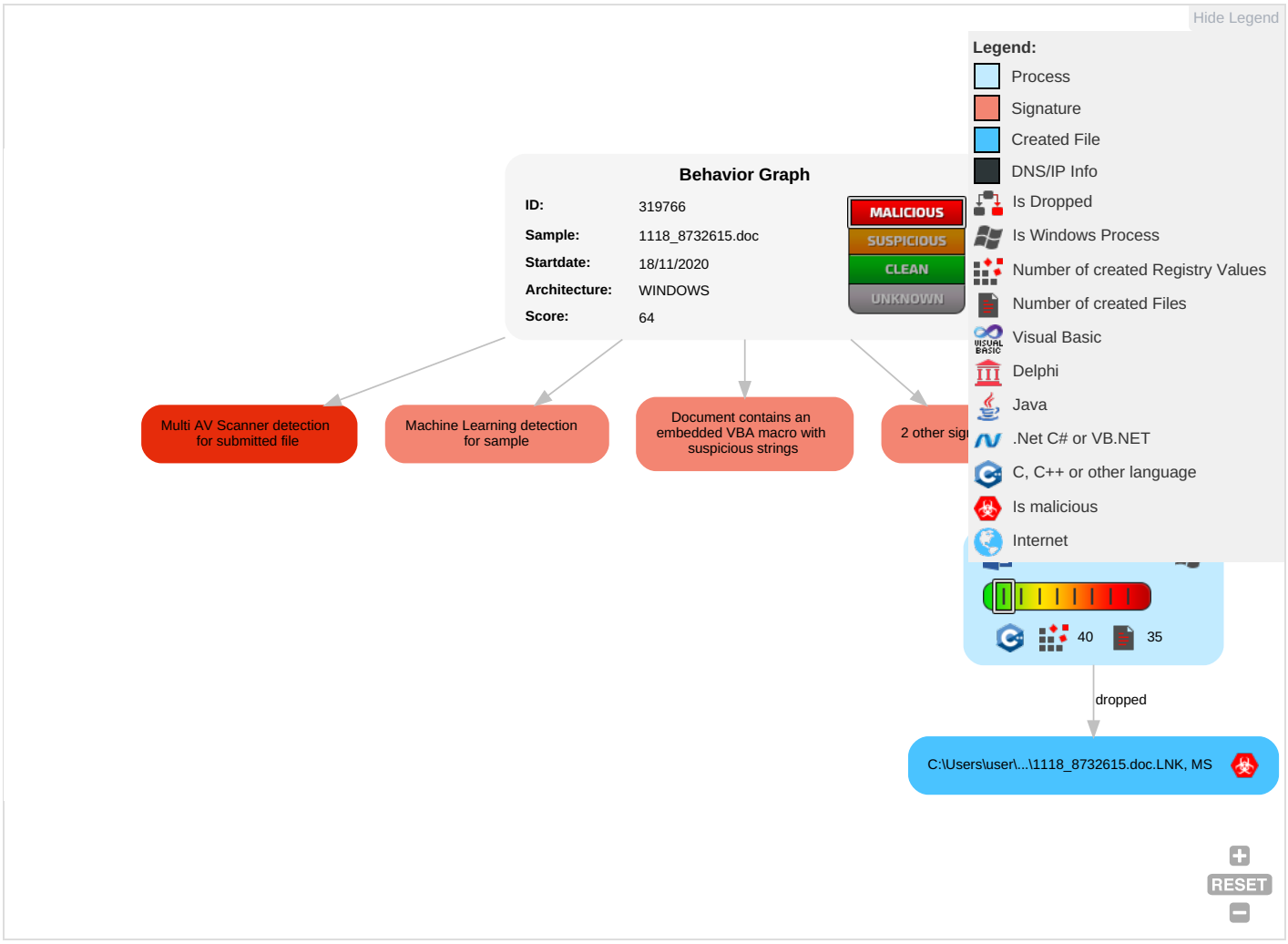
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

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 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 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

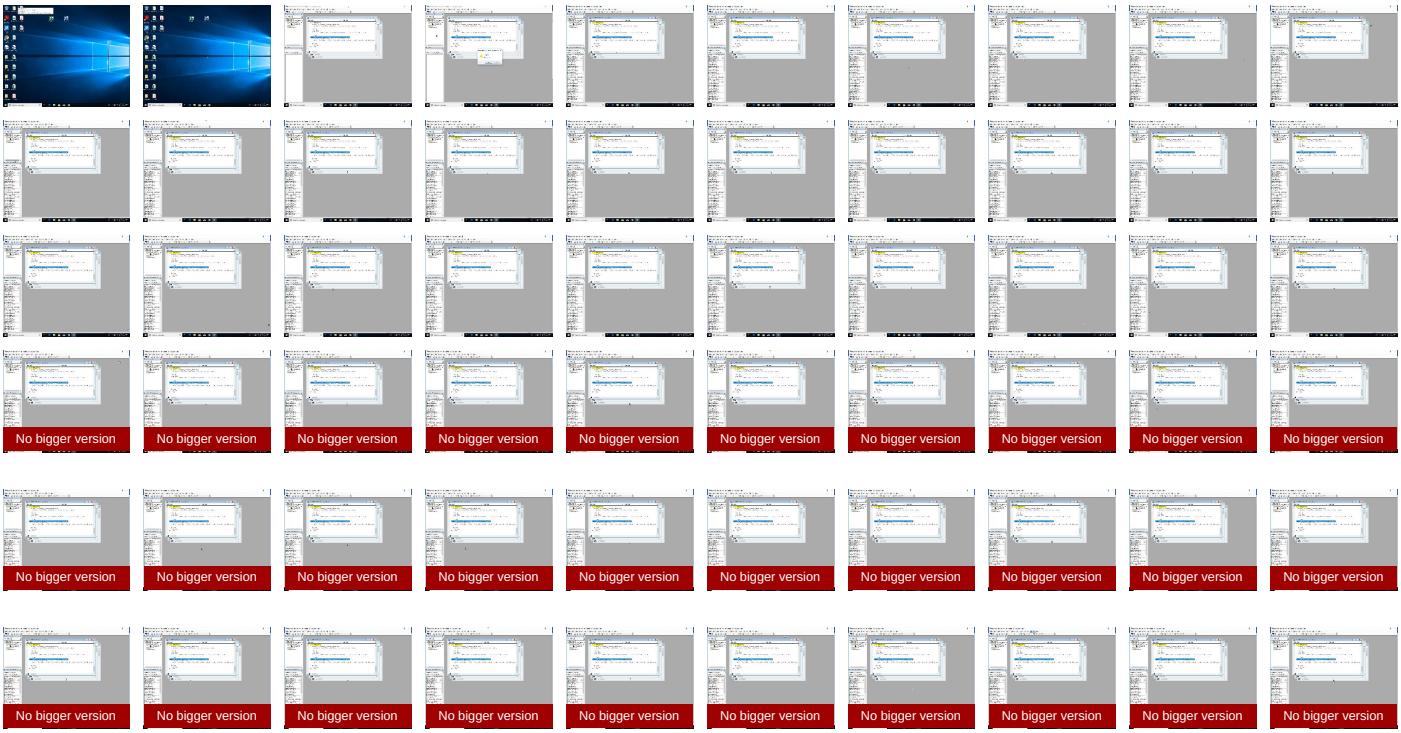
Behavior Graph

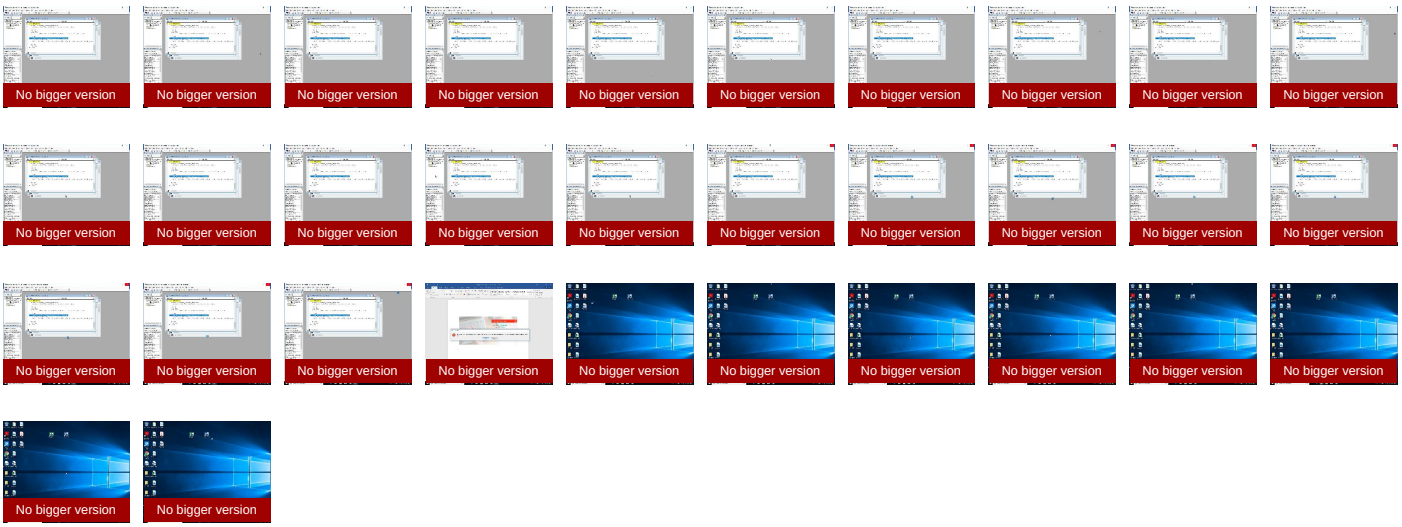


Screenshots

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
1118_8732615.doc	16%	Virustotal		Browse
1118_8732615.doc	12%	ReversingLabs	Script.Trojan.Wacatac	

Source	Detection	Scanner	Label	Link
1118_8732615.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://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	

Source	Detection	Scanner	Label	Link
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	
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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://login.microsoftonline.com/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://shell.suite.office.com:1443	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://cdn.entity.	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://wus2-000.contentsync.	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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/tenantassociationkey	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://powerlift.acompli.net	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://cortana.ai	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://api.aadrm.com/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://api.microsoftstream.com/api/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://cr.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://graph.ppe.windows.net	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift-frontdesk.acompli.net	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://store.office.cn/addinstemplate	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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=	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://web.microsoftstream.com/video/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://graph.windows.net	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://dataservice.o365filtering.com/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://weather.service.msn.com/data.aspx	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://apis.live.net/v5.0/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://management.azure.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://outlook.office365.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://incidents.diagnostics.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://api.office.net	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://entitlement.diagnostics.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://autodiscover-s.outlook.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://templatelogging.office.com/client/log	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://management.azure.com/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://ncus-000.contentsync.	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://devnull.onenote.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://messaging.office.com/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://augloop.office.com/v2	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://skyapi.live.net/Activity/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://dataservice.o365filtering.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://directory.services.	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.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	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://onedrive.live.com/embed?	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://augloop.office.com	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319766
Start date:	18.11.2020
Start time:	16:22:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1118_8732615.doc
Cookbook file name:	default.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
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.winDOC@1/7@0/0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.122.171.231, 168.61.161.212, 52.109.76.6, 52.109.76.36, 52.109.12.21, 51.11.168.160, 23.210.248.85, 205.185.216.42, 205.185.216.10, 20.54.26.129, 51.104.139.180, 92.122.213.194, 92.122.213.247, 52.155.217.156, 40.90.23.247, 40.90.23.206, 40.90.23.154, 40.90.23.153, 13.104.215.69, 13.104.215.72, 40.90.137.126, 40.90.137.127, 40.127.240.158, 51.11.168.232 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, cds.d2s7q6s2.hwcdn.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skypedataprdcolcus07.cloudapp.net, config.officeapps.live.com, europe.configsvc1.live.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found.
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\3EBA6D72-689F-46F1-A58C-F50E3BD4CDEC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378331924167014
Encrypted:	false
SSDEEP:	1536:tcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:PmQ9DQW+zBX8u
MD5:	4C5D6BFCD462D9677EBB3EDB85DFF67B
SHA1:	C74E656C67C9B90D62FDBDB2F38ADD48478A019B
SHA-256:	70BC1689EBA0C8647E2E344A9E0B0A0D2BA355C564B68DEC49F820C59649A100
SHA-512:	8A831AA4E0C172A23B9C7D852EA52C09D1C5CA3DBBDFC0FDC3275E2CA68A4F1174ECB73CA6AC306BF9C34602E4980B2BD2CCB1FE012D4FD84F54D6093A89 2B0
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="2020-11-18T15:23:50">.. Build: 16.0.13515.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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.MSO\4FAE44D.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	modified
Size (bytes):	5416
Entropy (8bit):	2.0520805575447705
Encrypted:	false
SSDEEP:	24:YISOayKbfoyVbs/qpBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBBBBBBBUBBBBBBqBJ:HVmbfogbsU07wgNgXalj+JL
MD5:	5F98F862F370C31BD4AB71F758D11B14
SHA1:	44221D1E056B5DB2C8EF8197CDE763F194A4657C
SHA-256:	4F529AA95102406D4A45B29D7B418D2402817795602DCAE4A5F24C95E2123568
SHA-512:	6DBE30CBE0BAACE1FBC5804E738B8ECBB1CABFD8E90D1FC0806F4EEBD23524E1E7CDE15E33EC8CE5C77ED0D88DB47F4BD288E749B0EE3507066FFCE95A1 3E8B0
Malicious:	false
Reputation:	low
Preview:	....l... .....D..... EMF....(.....V.....i.....:.....M...$...#.....B... ...#..... ... .?.....?.....l...0..... ... ...(... ...".. .....?.....3...7...7...?.M.....#.....B... ...#..... ... ...F.f.....?.....?..... .....l...4..... ... ...(... ... .

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{58EC7C29-FC88-4CA2-A6C0-9123E4D0B0C9}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{58EC7C29-FC88-4CA2-A6C0-9123E4D0B0C9}.tmp	
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\Office\Recent\1118_8732615.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Wed Nov 18 23:23:50 2020, atime=Wed Nov 18 23:23:47 2020, length=621568, window=hide
Category:	dropped
Size (bytes):	2130
Entropy (8bit):	4.673135614679704
Encrypted:	false
SSDEEP:	24:83O5j/7ShIK+AkW4D/W7aB6my3O5j/7ShIK+AkW4D/W7aB6m:83onSIOkWefB6p3onSIOkWefB6
MD5:	6276BFEA591D8E37F6133FE9552DCF60
SHA1:	BDE7914CD7675152B412A1DF97C3D203C7D61950
SHA-256:	542298C8D97CEFE32A72BBF0AC7098B0EDFEDF78618CC496DA4A6CF1BFDD8369
SHA-512:	7A8E66324467B218B3F803D3FC3FD12E18D3D070C5074BFFB8F5EB49C8394CB51596E21FC224A29DE86B978FA02DFE7944C7878FDF353F2596E54CEDA82B146
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... ...g-m.:.....@.....?.....|.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..sQ.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.sQ.....S.....J.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.sQ.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....n.2..|..sQ.. .1118_8~1.DOC..R.....>QuxsQ.....h.....y#..1.1.1.8._.8.7.3.2.6.1.5...d.o.c.....V.....-.....U.....>.S.....C:\Users\user\Desktop\1118_8732615.doc..'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.1.1.1.8._.8.7.3.2.6.1.5...d.o.c.....:..,.LB.)...As...`.....X.....724536.....!a..%.H.VZAj...T..-.....-..!a..%.H.VZAj...T..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.235670976640587
Encrypted:	false
SSDEEP:	3:M1UUvlLBC+dclLBCmX1UUvlLBCv:Mea9py92a9s
MD5:	F474223C2C879253F9A638B2D9E53BA6
SHA1:	26645E4A3856BD5C8FEF7664B98E6A89E0FB20D3
SHA-256:	6A1D2784F2E8DE87D55A5095EFE10C2B588B0E475CDDEA9F679064BACFD966DF
SHA-512:	B113B497E5801661DEA171F60660C3A304F813A892512B70A92F1DA077096D9E175AB5CD3486809F8EC36AE557A652C34EE463D479E9A70D1D04EF51F5751DEF
Malicious:	false
Reputation:	low
Preview:	[doc]..1118_8732615.doc.LNK=0..1118_8732615.doc.LNK=0..[doc]..1118_8732615.doc.LNK=0..

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):	2.1073706520881803
Encrypted:	false
SSDEEP:	3:Rl/Zd/btMztvtlbFzflqKmyl1/5:RtZ9+zxWA1B
MD5:	9412CC0321BD5F055E6E6356E461865C
SHA1:	870ECAFD5EC499D628DA7C40DE5DDA7077D69B5C
SHA-256:	695A224B4078A4C81952EDBD75B4CC015EE6E7E7B873674EF9B80CDEF9B87A59

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
SHA-512:	EC88BF93954204C0A479CCE1DCFF42572FCA0C6A3EF713E35386CCAE16E554BB2CADC18E59578A23398E17418B884BB95D1F73BF2040C7C17AA15447B669C4 0
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....H.....6C.....$...

C:\Users\user\Desktop\~$18_8732615.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1073706520881803
Encrypted:	false
SSDEEP:	3:Rl/Zd/btMztvtlbFzflqKmyl1/5:RtZ9+zxWA1B
MD5:	9412CC0321BD5F055E6E6356E461865C
SHA1:	870ECAFD5EC499D628DA7C40DE5DDA7077D69B5C
SHA-256:	695A224B4078A4C81952EDBD75B4CC015EE6E7E7B873674EF9B80CDEF9B87A59
SHA-512:	EC88BF93954204C0A479CCE1DCFF42572FCA0C6A3EF713E35386CCAE16E554BB2CADC18E59578A23398E17418B884BB95D1F73BF2040C7C17AA15447B669C4 0
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....H.....6C.....$...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: BigAdministrator, Template: Normal.dotm, Last Saved By: BigAdministrator, Revision Number: 56, Name of Creating Application: Microsoft Office Word, Total Ed iting Time: 44:00, Create Time/Date: Thu Nov 12 08 :27:00 2020, Last Saved Time/Date: Wed Nov 18 10:2 6:00 2020, Number of Pages: 1, Number of Words: 3, Number of Characters: 19, Security: 0
Entropy (8bit):	6.608390292496962
TrID:	• Perfect Keyboard macro set (36024/1) 37.90% • Microsoft Word document (32009/1) 33.68% • Microsoft Word document (old ver.) (19008/1) 20.00% • Generic OLE2 / Multistream Compound File (8008/1) 8.43%
File name:	1118_8732615.doc
File size:	619520
MD5:	0f75ad40daec01aee7642795cc544bb3
SHA1:	76334ccc6e92d579495671de47664180517cdf05
SHA256:	afba9deb16b5100c5964ca33cd42c2aa6b972ad104efd3d 58e0ad8b7070cd5f4
SHA512:	53bc11170d518dc95baddf223370398971f740830e24d9b 44b5e7bf61b99a3a62c680d3219bde489a5bb653629a3d 7669d022444161b5b2badc6c9d09b2fecd3
SSDEEP:	12288:9uE0gXPByytejpBOaFGyokkn7QljuI2hJdC3Zzo NSBr:9u3gXPQ2eXOaFefgCIn
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "1118_8732615.doc"

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:	
Subject:	
Author:	BigAdministrator
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	BigAdministrator
Revion Number:	56
Total Edit Time:	2640
Create Time:	2020-11-12 08:27:00
Last Saved Time:	2020-11-18 10:26:00
Number of Pages:	1
Number of Words:	3
Number of Characters:	19
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:	1048576

Streams with VBA

VBA File Name: Module1.bas, Stream Size: 4151

General	
Stream Path:	Macros/VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	4151
Data ASCII:	. . . . B . . . . p . . . 4 . . . . G . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 02 f0 00 00 00 42 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 70 05 00 00 34 0d 00 00 00 00 00 00 01 00 00 00 47 91 94 e0 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 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

VBA Code Keywords

Keyword
lka(UUu
Object
"al\Te"
VB_Name
vbDirectory)
"Loc"
"mp",
RootPath
zxc(afs)
Getme(Left(ActiveDocument.AttachedTemplate.Path,
String
ActiveDocument.AttachedTemplate.Path
String)
Selection.TypeBackspace
Nothing
myArr
ntgs)
lka(RootPath)
fld.SUBFOLDERS
Getme(RootPath
"Local\Temp")
While
ssss()
Function
CreateObject("Scripting.FileSystemObject")
Dir(RootPath
Getme(vhhs.Path)
Dir(Left(ActiveDocument.AttachedTemplate.Path,
Attribute
fso.GetFolder(asdf)
Getme
strFileExists
Dir(ActiveDocument.AttachedTemplate.Path

VBA Code

VBA File Name: Module2.bas, Stream Size: 2129

General	
Stream Path:	Macros/VBA/Module2
VBA File Name:	Module2.bas
Stream Size:	2129
Data ASCII:	. . . . . G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 0a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 11 03 00 00 dd 06 00 00 00 00 00 00 01 00 00 00 47 91 03 f5 00 00 ff ff 03 00 00 00 00 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 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Unit:=wdCharacter,
Dir(sf
VB_Name
ActiveDocument.AttachedTemplate.Path
String)
Selection.TypeBackspace
Unit:=wdLine,
strFileExists
Selection.Copy
zxc(sf
Selection.MoveRight

Keyword
Attribute
Selection.MoveDown
Dir(ActiveDocument.AttachedTemplate.Path

VBA Code

VBA File Name: ThisDocument.cls, Stream Size: 1743

General	
Stream Path:	Macros/VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1743
Data ASCII:	. . . . T . . . . \\ . . . H . . . . G . . n . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 01 f0 00 00 00 54 03 00 00 d4 00 00 00 e2 01 00 00 ff ff ff ff 5c 03 00 00 48 05 00 00 00 00 00 00 01 00 00 00 47 91 f2 6e 00 00 ff ff a3 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

VBA Code Keywords

Keyword
VB_Name
VB_Creatable
VB_Exposed
AutoOpen()
VB_Customizable
a.ShellExecute("rund"
VB_TemplateDerived
"ThisDocument"
False
Attribute
Dir(ActiveDocument.AttachedTemplate.Path
VB_PredeclaredId
VB_GlobalNameSpace
SW_SHOWNORMAL)
VB_Base
Scr_hDC
ActiveDocument.AttachedTemplate.Path

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
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 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: 280

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data

General	
Stream Size:	280
Entropy:	2.3837065211
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . h . . . . . p . . . . . | . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 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 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 436

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	436
Entropy:	3.43041331515
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . L . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . B i g A d m i n i s t r a t o r . . . . .
Data Raw:	fe ff 00 00 0a 00 02 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 84 01 00 00 11 00 00 00 01 00 00 00 90 00 00 00 02 00 00 00 98 00 00 00 03 00 00 00 a4 00 00 00 04 00 00 00 b0 00 00 00 05 00 00 00 cc 00 00 00 06 00 00 00 d8 00 00 00 07 00 00 00 e4 00 00 00 08 00 00 00 f8 00 00 00 09 00 00 00 14 01 00 00

Stream Path: 1Table, File Type: ARC archive data, crunched, Stream Size: 7940

General	
Stream Path:	1Table
File Type:	ARC archive data, crunched
Stream Size:	7940
Entropy:	5.90771618128
Base64 Encoded:	True
Data ASCII:	. . . . . w . . . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . v . . . 6 . . . 6 . . . 6 . . . 6 . . . 6 . . . > . . . 6 . . .
Data Raw:	1a 06 0f 00 12 00 01 00 77 01 0f 00 07 00 03 00 03 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 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 76 02 00 00

Stream Path: Data, File Type: data, Stream Size: 129034

General	
Stream Path:	Data
File Type:	data
Stream Size:	129034
Entropy:	7.75936836126
Base64 Encoded:	True
Data ASCII:	7 . . . D . d . . . . . $ . . . . . ~ . . . . . s . . . Z . . . . A . . . . . ? . . . . . 2 . 0 . 2 . 0 . _ . 2 . . . P . i . c . t . u . r . e . . 1 . . . 2 . 0 . 2 . 0 . _ . 2 . . . . . R . . . e . . . . . b b . . o . . k . 1 . U . { . . . A . . . . . D . . . . . p z . F . . 9 . . . . b
Data Raw:	37 f3 01 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 9f 24 da 16 e8 03 e8 03 00 00 00 00 00 00 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 7e 00 00 00 b2 04 0a f0 08 00 00 00 01 04 00 00 00 0a 00 00 00 73 00 0b f0 5a 00 00 00 04 41 01 00 00 00 05 c1 0e 00 00 00 ff 01 00 00 08 00 3f 03 10 00 10 00 80 c3 14 00

Stream Path: Macros/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 459

General	
Stream Path:	Macros/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	459
Entropy:	5.38318286733

General	
Base64 Encoded:	True
Data ASCII:	I D = " { 1 1 0 A 9 F D 0 - A 4 8 D - 4 3 4 6 - B D 2 3 - C D 9 3 8 7 2 F 3 4 6 8 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . M o d u l e = M o d u l e 2 . . 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 = " 8 5 8 7 4 B 7 1 4 B 9 1 4 F 9 1 4 F 9 1 4 F 9 1 4 F " . . D P B = " A 9 A B 6 7 7 8 6 8 7 8 6 8 7 8 " . . G C = " C D C F 0 3 B 9 0 3 D C 0 4 D
Data Raw:	49 44 3d 22 7b 31 31 30 41 39 46 44 30 2d 41 34 38 44 2d 34 33 34 36 2d 42 44 32 33 2d 43 44 39 33 38 37 32 46 33 34 36 38 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 32 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48

Stream Path: Macros/PROJECTwm, File Type: data, Stream Size: 89

General	
Stream Path:	Macros/PROJECTwm
File Type:	data
Stream Size:	89
Entropy:	3.27035029005
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . M o d u l e 2 . M . o . d . u . l . e . 2 . . . . .
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 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 4d 6f 64 75 6c 65 32 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 32 00 00 00 00 00

Stream Path: Macros/VBA/_VBA_PROJECT, File Type: data, Stream Size: 3484

General	
Stream Path:	Macros/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3484
Entropy:	4.50229327005
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 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 . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 06 00 02 00 20 01 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 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 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: Macros/VBA/dir, File Type: data, Stream Size: 703

General	
Stream Path:	Macros/VBA/dir
File Type:	data
Stream Size:	703
Entropy:	6.40700107529
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . 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 t e m 3 . 2 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . * . \\ C . . . . * . . a .
Data Raw:	01 bb b2 80 01 00 04 00 00 00 03 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 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 14 08 06 12 09 02 12 80 a1 cd a2 61 0a 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: ObjectPool/_1667171533/\x1CompObj, File Type: data, Stream Size: 76

General	
Stream Path:	ObjectPool/_1667171533/\x1CompObj
File Type:	data
Stream Size:	76
Entropy:	3.09344952647
Base64 Encoded:	False
Data ASCII:	. . . . F . . . . O L E P a c k a g e . . . . P a c k a g e . . 9 . q . . . .

General	
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 0c 00 03 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 0c 00 00 00 4f 4c 45 20 50 61 63 6b 61 67 65 00 00 00 00 08 00 00 00 50 61 63 6b 61 67 65 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: ObjectPool/_1667171533/\x1Ole10Native, File Type: data, Stream Size: 453046

General	
Stream Path:	ObjectPool/_1667171533/\x1Ole10Native
File Type:	data
Stream Size:	453046
Entropy:	6.15758899612
Base64 Encoded:	True
Data ASCII:	. . . . . 2 2 . m p 4 . C : \\ U s e r s \\ B i g A d m i n i s t r a t o r \\ A p p D a t a \\ L o c a l \\ M i c r o s o f t \\ W i n d o w s \\ I N e t C a c h e \\ C o n t e n t . M S O \\ 2 2 . m p 4 . . . . . , . . . C : \\ U s e r s \\ B I G A D M ~ 1 \\ A p p D a t a \\ L o c a l \\ T e m p \\ 2 2 . m p 4 . . . . . M Z . . . . . @ . . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e
Data Raw:	b2 e9 06 00 02 00 32 32 2e 6d 70 34 00 43 3a 5c 55 73 65 72 73 5c 42 69 67 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 49 4e 65 74 43 61 63 68 65 5c 43 6f 6e 74 65 6e 74 2e 4d 53 4f 5c 32 32 2e 6d 70 34 00 00 00 03 00 2c 00 00 00 43 3a 5c 55 73 65 72 73 5c 42 49 47 41 44 4d 7e 31 5c 41 70

Stream Path: ObjectPool/_1667171533/\x3ObjInfo, File Type: data, Stream Size: 6

General	
Stream Path:	ObjectPool/_1667171533/\x3ObjInfo
File Type:	data
Stream Size:	6
Entropy:	1.79248125036
Base64 Encoded:	False
Data ASCII:	@ . . . . .
Data Raw:	40 00 03 00 01 00

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

General	
Stream Path:	WordDocument
File Type:	data
Stream Size:	4096
Entropy:	1.58736027199
Base64 Encoded:	False
Data ASCII:	. . . . Y . . . . . b j b j 8 . 8 . . . . . Z p . e Z p . e . . . . . B . . . . . B . . . . .
Data Raw:	ec a5 c1 00 59 00 09 04 00 00 f8 12 bf 00 00 00 00 00 00 10 00 00 00 00 00 08 00 00 16 08 00 00 0e 00 62 6a 62 6a 38 1a 38 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 04 16 00 2e 0e 00 00 5a 70 d2 65 5a 70 d2 65 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
Nov 18, 2020 16:23:44.672111988 CET	60831	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:44.699354887 CET	53	60831	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:45.734983921 CET	60100	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:45.762037992 CET	53	60100	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:46.561341047 CET	53195	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:46.596785069 CET	53	53195	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:47.481641054 CET	50141	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:47.517193079 CET	53	50141	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:48.716761112 CET	53023	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:48.743879080 CET	53	53023	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:23:49.673250914 CET	49563	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:49.700500965 CET	53	49563	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:49.967376947 CET	51352	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:50.002960920 CET	53	51352	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:50.513377905 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:50.550532103 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:51.519773006 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:51.556525946 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:52.535950899 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:52.571599007 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:53.249342918 CET	57084	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:53.276588917 CET	53	57084	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:54.062916994 CET	58823	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:54.090373039 CET	53	58823	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:54.552730083 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:54.588104963 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:54.873327971 CET	57568	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:54.900521994 CET	53	57568	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:55.744959116 CET	50540	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:55.772099018 CET	53	50540	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:56.575012922 CET	54366	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:56.602183104 CET	53	54366	8.8.8.8	192.168.2.3
Nov 18, 2020 16:23:58.573808908 CET	59349	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:23:58.609177113 CET	53	59349	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:10.710871935 CET	53034	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:10.737885952 CET	53	53034	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:16.322771072 CET	57762	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:16.358537912 CET	53	57762	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:32.313694000 CET	55435	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:32.349092960 CET	53	55435	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:33.835822105 CET	50713	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:33.871289015 CET	53	50713	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:48.684983015 CET	56132	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:48.712060928 CET	53	56132	8.8.8.8	192.168.2.3
Nov 18, 2020 16:24:52.870249033 CET	58987	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:24:52.907192945 CET	53	58987	8.8.8.8	192.168.2.3
Nov 18, 2020 16:25:30.357062101 CET	56579	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:25:30.384232044 CET	53	56579	8.8.8.8	192.168.2.3
Nov 18, 2020 16:25:33.563417912 CET	60633	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:25:33.590511084 CET	53	60633	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:38.822729111 CET	61292	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:38.858268976 CET	53	61292	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:39.382054090 CET	63619	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:39.417794943 CET	53	63619	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:39.850081921 CET	64938	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:39.885713100 CET	53	64938	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:40.193862915 CET	61946	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:40.229302883 CET	53	61946	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:40.656085968 CET	64910	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:40.683223009 CET	53	64910	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:41.181739092 CET	52123	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:41.219552994 CET	53	52123	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:41.848578930 CET	56130	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:41.875646114 CET	53	56130	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:42.596065998 CET	56338	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:42.632189035 CET	53	56338	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:43.354547977 CET	59420	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:43.381690025 CET	53	59420	8.8.8.8	192.168.2.3
Nov 18, 2020 16:26:43.723516941 CET	58784	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:26:43.761198997 CET	53	58784	8.8.8.8	192.168.2.3
Nov 18, 2020 16:28:32.424343109 CET	63978	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:28:32.459765911 CET	53	63978	8.8.8.8	192.168.2.3
Nov 18, 2020 16:28:33.076272964 CET	62938	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:28:33.111910105 CET	53	62938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 16:28:36.854615927 CET	55708	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:28:36.898546934 CET	53	55708	8.8.8.8	192.168.2.3
Nov 18, 2020 16:28:42.821544886 CET	56803	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:28:42.857161045 CET	53	56803	8.8.8.8	192.168.2.3
Nov 18, 2020 16:28:43.086266041 CET	57145	53	192.168.2.3	8.8.8.8
Nov 18, 2020 16:28:43.121985912 CET	53	57145	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2440 Parent PID: 792

General

Start time:	16:23:47
Start date:	18/11/2020
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:	0x1d0000
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 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	66AD977C	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	669D765D	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	669D765D	unknown

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\1118_8732615.doc	0	24	success or wait	1	669FAA87	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66A18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	success or wait	1	66A05805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E6009040000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1366425601	success or wait	1	66A77FEE	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Recognizers\{3133A7FE-BC5F-4D81-BF02-184ECC88D66E}	NULL	unicode		success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	NULL	unicode		success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{16A933D2-A296-49D5-96FC-C7C2DAEE88B4}	filename	unicode	C:\PROGRA~2\COMMON~1\MICROS~1\SMARTT~1\LISTS\BASMLA.XSL	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{3CC385AC-95CC-4A75-BF35-AB36AE645BCF}	NULL	unicode		success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{99E0D1EC-0A0D-4E50-B8A1-82A8B6ECE5CB}	NULL	unicode		success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Actions\{B7EFF951-E52F-45CC-9EF7-57124F2177CC}	Solution	unicode	{15727DE6-F92D-4E46-ACB4-0E2C58B31A18}	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag	migratedBitValues	binary	01 00 00 00	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	FriendlyName	unicode	Microsoft Word 16.0	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	Save	binary	01 00 00 00	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowButtons	binary	01 00 00 00	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Smart Tag\Applications\OpusApp	ShowIndicators	binary	01 00 00 00	success or wait	1	66A05805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1366425601	success or wait	1	669D765D	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	ProductNonBootFilesIntl_1033	dword	1366425601	1366425602	success or wait	1	669D765D	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word	WordName	unicode	Word	Word (Unlicensed Product)	success or wait	1	669D765D	unknown

Disassembly