

JOeSandbox Cloud BASIC



ID: 635245

Sample Name: INVOICE.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 17:49:26

Date: 27/05/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report INVOICE.doc	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Initial Sample	3
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	4
AV Detection	4
Exploits	4
Software Vulnerabilities	4
System Summary	4
Mitre Att&ck Matrix	4
Behavior Graph	5
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	7
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
World Map of Contacted IPs	10
General Information	10
Warnings	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASNs	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\55500104-7BA4-450F-B5B6-9FAE4E02D958	11
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.Word\~WRS{182A308B-3928-43D2-96AF-DFBDD8FBB8}.tmp	12
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.Word\~WRS{E6ECC2FB-A299-4715-927D-C678F6A7F37A}.tmp	12
C:\Users\user\AppData\Local\Temp\Client.exe	12
C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier	13
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INVOICE.doc.LNK	13
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	13
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	13
C:\Users\user\Desktop\~\$NVOICE.doc	14
Static File Info	14
General	14
File Icon	14
Static RTF Info	14
Objects	14
Network Behavior	15
Statistics	15
System Behavior	15
Analysis Process: WINWORD.EXE PID: 6412, Parent PID: 756	15
General	15
File Activities	15
File Created	15
File Deleted	15
Registry Activities	15
Key Created	15
Key Value Created	16
Key Value Modified	17
Disassembly	20

Windows Analysis Report

INVOICE.doc

Overview

General Information

Sample Name:

INVOICE.doc

Analysis ID:

635245

MD5:

0ecb6ed891d173..

SHA1:

6867f37817db50..

SHA256:

f080b3ba979f854..

Tags:

doc

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Document exploit detected (creates...

Multi AV Scanner detection for subm...

Document exploit detected (drops P...

Malicious sample detected (through...

Multi AV Scanner detection for drop...

Office process drops PE file

PE file has nameless sections

Machine Learning detection for drop...

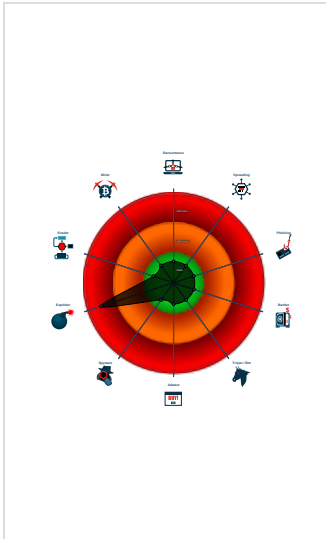
Found suspicious RTF objects

Found potential equation exploit (CV...

Yara signature match

PE file contains strange resources

Classification



Process Tree

- System is w10x64
- WINWORD.EXE (PID: 6412 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
INVOICE.doc	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	<ul style="list-style-type: none">0x177f:\$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f64650x16e3:\$m1: 4d5a90000300000004000000ffff
INVOICE.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit documents.	ditekSHen	<ul style="list-style-type: none">0x1269:\$obj2: \objdata0x207214:\$obj2: \objdata0x3e240c:\$obj3: \objupdate0x8de:\$obj4: \objemb0x206889:\$obj4: \objemb

Sigma Signatures

 No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits



Found potential equation exploit (CVE-2017-11882)

Software Vulnerabilities



Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

System Summary



Malicious sample detected (through community Yara rule)

Office process drops PE file

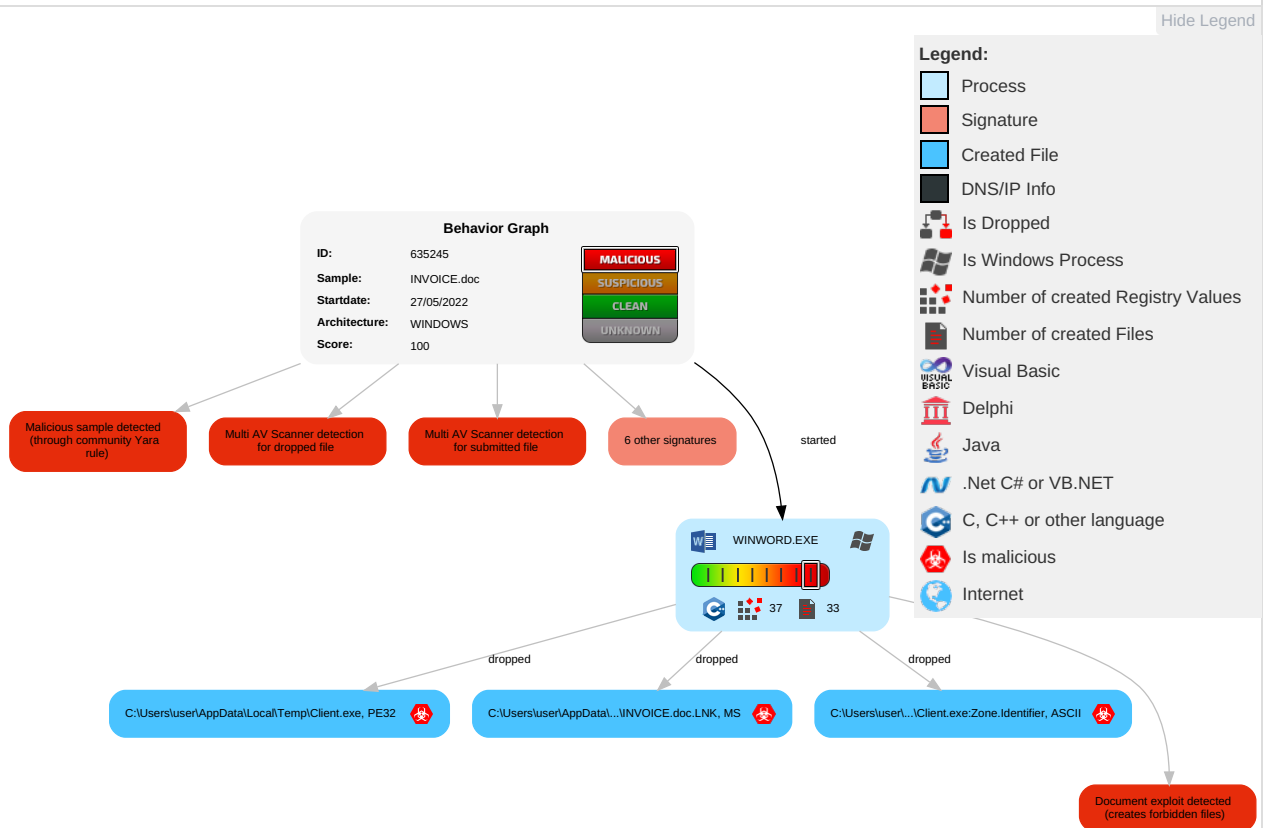
PE file has nameless sections

Found suspicious RTF objects

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	3 Exploitation for Client Execution	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	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	2 Software Packing	LSASS Memory	1 File and Directory Discovery	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Obfuscated Files or Information	Security Account Manager	2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

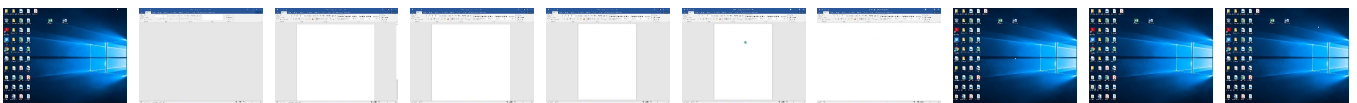
Behavior Graph

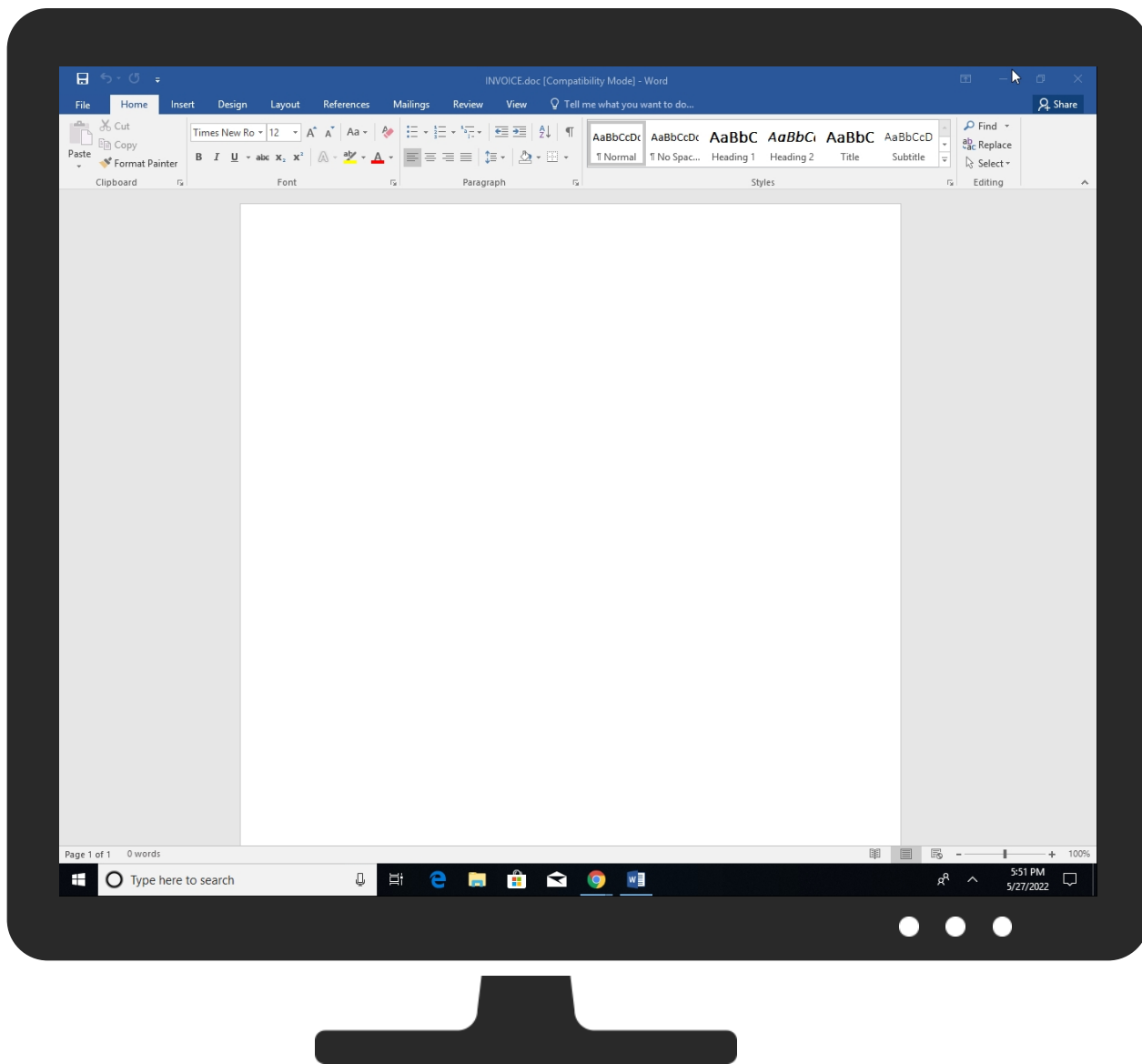


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
INVOICE.doc	50%	Virustotal		Browse
INVOICE.doc	20%	ReversingLabs	Document-RTF.Trojan.Injuke	


Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Client.exe	63%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Client.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Client.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.RealP roTECT	


Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	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://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	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.diagnosticsrdf.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://login.microsoftonline.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://shell.suite.office.com:1443	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://autodiscover-s.outlook.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://roaming.edog.	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://cdn.entity.	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://api.addins.omex.office.net/appinfo/query	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://powerlift.acompli.net	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rpsticket.partnerservices.getmicrosoftkey.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://cortana.ai	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://entitlement.diagnosticsdf.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.aadrm.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.microsoftstream.com/api/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://cr.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	low
http://https://portal.office.com/account/?ref=ClientMeControl	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://graph.ppe.windows.net	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://powerlift-frontdesk.acompli.net	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://tasks.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://store.office.cn/addinstemplate	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://api.aadrm.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://messaging.engagement.office.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://www.odwebp.svc.ms	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://api.diagnosticsdf.office.com/v2/feedback	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://web.microsoftstream.com/video/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://graph.windows.net	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dataservice.o365filtering.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://officesetup.getmicrosoftkey.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://analysis.windows.net/powerbi/api	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	<ul style="list-style-type: none"> URL Reputation: safe 	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://powerpoint.uservice.com/forums/288952-powerpoint-for-ipad-iphone-ios	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://ncus.contentsync	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscover/service.svc/root/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://weather.service.msn.com/data.aspx	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://apis.live.net/v5.0/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://autodiscover.s.outlook.com/autodiscover/autodiscover.xml	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://management.azure.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://outlook.office365.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://wus2.contentsync	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.office.net	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://incidents.diagnosticsdf.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://asgmsproxyapi.azurewebsites.net/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://entitlement.diagnostics.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://outlook.office.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://outlook.office365.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://webshell.suite.office.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://substrate.office.com/search/api/v1/SearchHistory	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://management.azure.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://devnull.onenote.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://ncus.pagecontentsync	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://messaging.office.com/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://augloop.office.com/v2	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://skyapi.live.net/Activity/	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false		high
http://https://dataservice.o365filtering.com	55500104-7BA4-450F-B5B6-9FAE4E02D958.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635245
Start date and time: 27/05/202217:49:26	2022-05-27 17:49:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.doc
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:	25
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.winDOC@1/9@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">• Found application associated with file extension: .doc• Adjust boot time• Enable AMSI• Found Word or Excel or PowerPoint or XPS Viewer• Attach to Office via COM• Scroll down• Close Viewer


Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrivSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.109.88.177, 52.109.12.22, 52.109.76.34
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prod-w.nexus.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, config.officeapps.live.com, sls.update.microsoft.com, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, officeclient.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, europe.configsvc1.live.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

- Report size getting too big, too many NtSetInformationFile calls found.


Simulations

Behavior and APIs


 No simulations

Joe Sandbox View / Context


IPs

 No context


Domains

 No context


ASNs

 No context

JA3 Fingerprints

 No context

Dropped Files

 No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\55500104-7BA4-450F-B5B6-9FAE4E02D958

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):	147717
Entropy (8bit):	5.359207546988477
Encrypted:	false
SSDEEP:	1536:BcQW/gxgB5B3guw//Q9DQW+zQWk4F77nXmvidQXxUETLKz6e:dHQ9DQW+zIXLI
MD5:	E6E619CAC3C39DDB4DF743FBB9E139B8
SHA1:	F0328034164567F1678649AA8011D8CB0148FA43
SHA-256:	97C06E65DEDC51DC2BEE938FD6EDA3686C703A8D2B426651126407E9BA05EFCF
SHA-512:	F47CB2C0EEFF4D2484FC56E0999177A3D646EDF82E4DB9A89772B16DE27D08E906B037AA2A5A00C31E27FEB068CD98AECC91513EBE8ADB77DF922D0F3404EEBB
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="2022-05-27T15:50:41">.. Build: 16.0.15322.30526-->.. <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.aspx</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="CIViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="CIViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="CIViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L..Lg.b.....0..z.....@.....@.....O...@...}.....H.....VU3re.zH.....@....text....v....X......rsr c...}...@...~.....@..@.....`reloc.....@..B.....
----------	--

C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBC85A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443F98
Malicious:	true
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\INVOICE.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=Tue Mar 8 15:31:48 2022, mtime=Fri May 27 23:50:46 2022, atime=Fri May 27 23:50:35 2022, length=4073082, window=hide
Category:	dropped
Size (bytes):	1038
Entropy (8bit):	4.721773535285337
Encrypted:	false
SSDEEP:	12:8uOwFZtUFuEIPCH2GgDMcSYuM+WOHpfcmPHrvjAVWrDZ4vJUDs+JB5JT4t2Y+x4:8uN8DMPRcmfAVuHZ1DbBbh7aB6m
MD5:	3EA0F315A0A439B5E34C51407CD469C5
SHA1:	37D2487C125033E60E48C1267FACF8AB67D7DEC5
SHA-256:	2133D5285C52293619238103AC07FE60A8EDD1AA9B73DB4DC4265BE33CB46F68
SHA-512:	83F917140E924BDB678418E19856E22EAB15DF251C0E5E8B5046C88F1B8793BF195B860BE26E7D8C2FDE51CB1213C933D59C350B321AB942A9AF567DF5D767A
Malicious:	true
Preview:	L.....F.....3.....H,r.....1,r,z>.....P.O. :i.....+00../C:\.....x.1.....N....Users.d.....L...TK.....:.....q .U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,- .2.1.8.1.3.....P.1.....hT.....user.<.....Ny..TK.....S.....s...h.a.r.d.z.....~.1.....hT.....Desktop.h.....Ny..TK.....Y.....>.....Z....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,- 2.1.7.6.9.....b.2.z&>..TR. .INVOICE.doc.H.....hT...TR.....h.....b...I.N.V.O.I.C.E...d.o.c.....Q.....>.....P.....>.....S.....C:\Users\user\Desktop\INVOICE.do c..".....\.....\.....\D.e.s.k.t.o.p.\I.N.V.O.I.C.E...d.o.c.....;..LB.)...As..`.....X.....632922.....!a..%H.VZAj.....!a..%H.VZAj.....-.....1SPS.X F.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.....9...1SPS..mD..pH.H@..=x....

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):	73
Entropy (8bit):	4.614921998459085
Encrypted:	false
SSDEEP:	3:bDuMJl0XX1zCmX1KzqsX1zCv:bCPxEzqAxs
MD5:	5F789C623A9E8963E95B26CF07AFF5BF
SHA1:	7CD0106ECA31151951F4ADF9AFDB882DA0844F7B
SHA-256:	ACB5F625725B1D77B6E7C1466E32D4227A4A5925BD1B6AB9458B6D3BD9F113F3
SHA-512:	966205B839048F7D90578AD597D4684AC387D5CBDA125F14D71BD453C3D17F4FEDBC232F5F5AA71B009E33CF31987429F7D5EEF90F3E3F484CBEB7B1D2D2BBCE9A
Malicious:	false
Preview:	[folders]..Templates.LNK=0..INVOICE.doc.LNK=0..[doc]..INVOICE.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):	2.1150565317044543
Encrypted:	false
SSDEEP:	3:Rl/ZdAltHxolFVn8Xt7:RtZqdHoHS
MD5:	47F4DEA953CAF4684FDC3334445ACB04
SHA1:	C73E8ABB4806188C2DDF6FA5197CCD10E0743EAB
SHA-256:	EF91A0506BBAA9010B05BAAE67FD1165A83FD2705907EE01B67E3675279EF930
SHA-512:	402EF017DA02EF0B9F874C2697DF81BBC6E7A9164CED5D89CED82D6E523E5AA2EFC16529A96D165E119B11A134B5A70693DF58478C1BCD357CE655DC13FB58A4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....R:.....R>.E.....R2.5.....\$...

C:\Users\user\Desktop\~\$NVOICE.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.1150565317044543
Encrypted:	false
SSDEEP:	3:Rl/ZdAltHxolFVn8Xt7:RtZqdHoHS
MD5:	47F4DEA953CAF4684FDC3334445ACB04
SHA1:	C73E8ABB4806188C2DDF6FA5197CCD10E0743EAB
SHA-256:	EF91A0506BBAA9010B05BAAE67FD1165A83FD2705907EE01B67E3675279EF930
SHA-512:	402EF017DA02EF0B9F874C2697DF81BBC6E7A9164CED5D89CED82D6E523E5AA2EFC16529A96D165E119B11A134B5A70693DF58478C1BCD357CE655DC13FB58A4
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....R:.....R>.E.....R2.5.....\$...

Static File Info	
General	
File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	5.05599985084287
TrID:	<ul style="list-style-type: none">Rich Text Format (5005/1) 55.56%Rich Text Format (4004/1) 44.44%
File name:	INVOICE.doc
File size:	4073082
MD5:	0ecb6ed891d173443fa3654c31e14320
SHA1:	6867f37817db501ce103813f791899f3cf1bc1e8
SHA256:	f080b3ba979f854761526f4bc6bd5b8210b48d5f91f15b1a1423849107775e11
SHA512:	608f95fa01b0ecfc45f81f8b1e56539f08aae01f5589e7ce98f150e6e580eed1e39910f0b39596bff68b1ce338f9d2cfb6727287ad644ec64bdf34be2e65ac
SSDEEP:	24576:Z+h5y9IA8yaw1fba/f84V6FXjhHavKVp7Ai4q0LD33bqJXCJloYSUaJbjOpS/iqu:V
TLSH:	1616A431B13439D7C21F0435565FBD89430ABD83A3C66F8C518EFAF91EA69E7630690A
File Content Preview:	{\rtf1{*\pnseclvl3\pndec\pnstart1\pnindent720\pnhang {\pntxta .}}{*\pnseclvl4\pncltr\pnstart1\pnindent720\pnhang {\pntxta }}}{*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb ({\pntxta })}}{*\pnseclvl6\pncltr\pnstart1\pnindent720\pnhang {\pnt

File Icon	
	
Icon Hash:	74f4c4c6c1cac4d8

Static RTF Info
Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000128Dh	2	embedded	Package	1019559	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	00207238h	2	embedded	Equation.3	3072				no

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 6412, Parent PID: 756

General

Target ID:	0
Start time:	17:50:37
Start date:	27/05/2022
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:	0x800000
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	65AB977C	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$NVOICE.doc	success or wait	1	659E5805	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

