

ID: 321436
Sample Name:
acceptable_use_policy.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 05:57:14
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report acceptable_use_policy.docm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 19
General 19
File Icon 19
Static OLE Info 19
General 19
OLE File "/opt/package/joesandbox/database/analysis/321436/sample/acceptable_use_policy.docm" 19
Indicators 19
Summary 19
Document Summary 20
Streams with VBA 20
VBA File Name: ThisDocument.cls, Stream Size: 3038 20
General 20
VBA Code Keywords 20
VBA Code 21
Streams 21
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 366 21
General 21
Stream Path: PROJECTwm, File Type: data, Stream Size: 41 21
General 21
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2765 21

General 21
Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 1752 21
General 21
Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 102 22
General 22
Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 796 22
General 22
Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 103 22
General 22
Stream Path: VBA/dir, File Type: shared library, Stream Size: 520 22
General 22
Network Behavior 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 24
DNS Queries 25
DNS Answers 25
HTTPS Packets 25
Code Manipulations 26
Statistics 26
System Behavior 26
Analysis Process: WINWORD.EXE PID: 5360 Parent PID: 792 26
General 26
File Activities 26
File Created 26
Registry Activities 27
Key Created 27
Disassembly 28

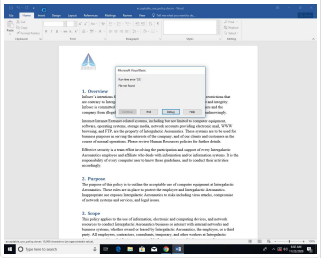
Analysis Report acceptable_use_policy.docm

Overview

General Information

Sample Name:	acceptable_use_policy.docm
Analysis ID:	321436
MD5:	d651d3331b60ee..
SHA1:	bb816e1502b0ba..
SHA256:	a0a9eca457bd72..

Most interesting Screenshot:



Detection

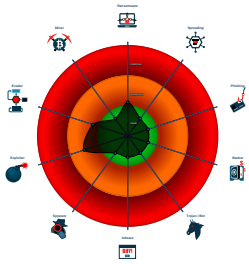


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Machine Learning detection for samp…
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Document contains no OLE stream …
- Document has an unknown applicati…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 5360 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

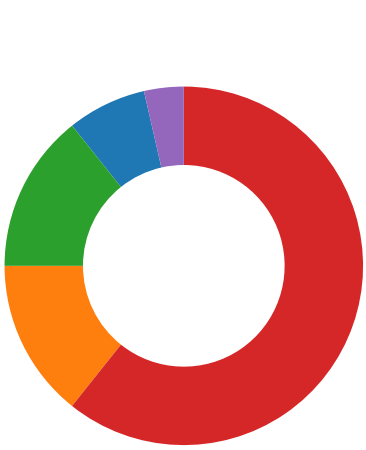
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection

Copyright null 2020



Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:



Document contains an embedded VBA macro which may execute processes

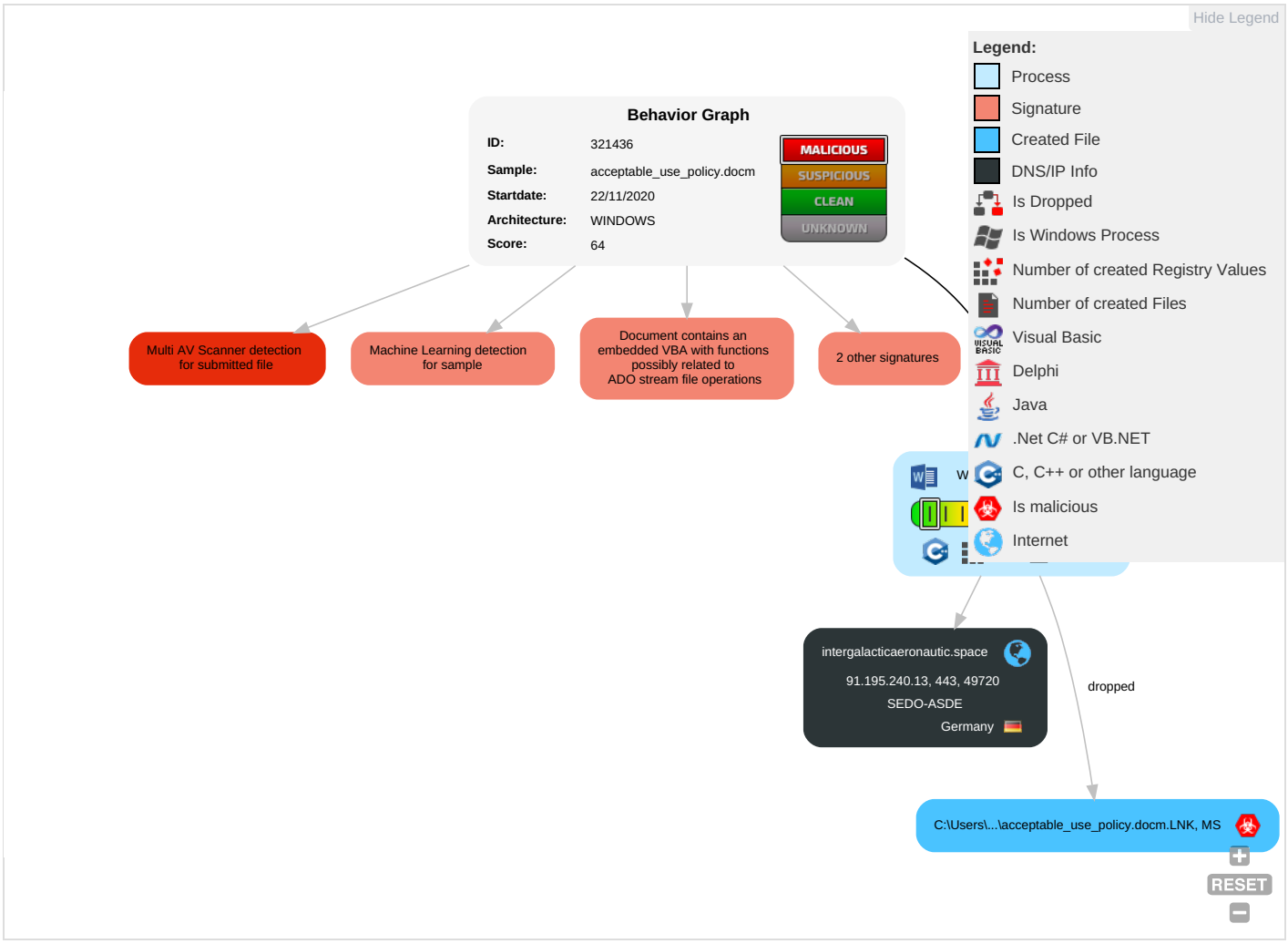
Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA with functions possibly related to HTTP operations

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Imp
Valid Accounts	Scripting 3 2	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Exploitation for Client Execution 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 3 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

Behavior Graph

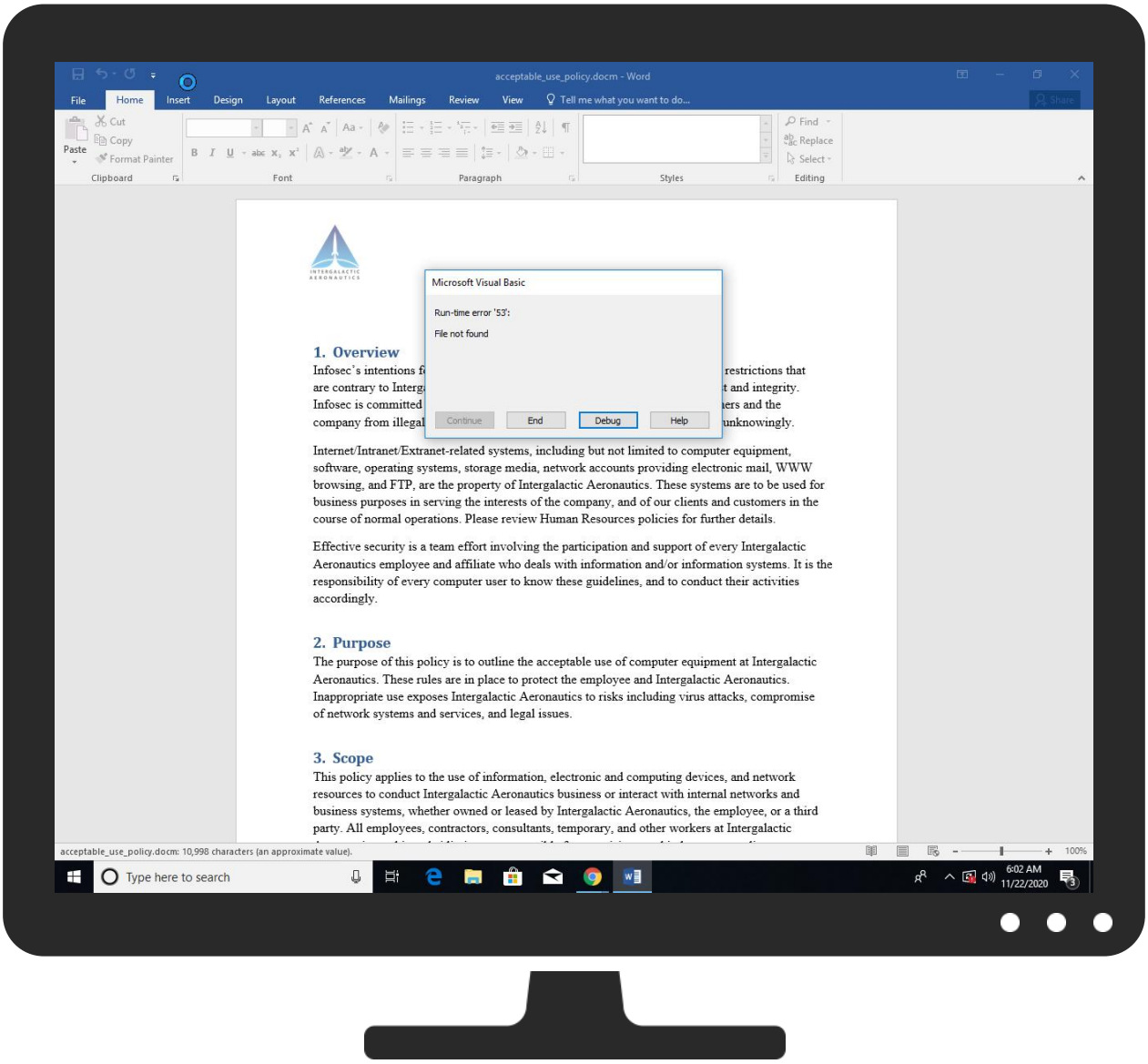


Screenshots

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
acceptable_use_policy.docm	60%	Virustotal		Browse
acceptable_use_policy.docm	48%	ReversingLabs	Script.Downloader.Obfuser	
acceptable_use_policy.docm	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
intergalacticaeronautic.space	0%	Virustotal		Browse

URLs

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

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://intergalacticaeronautic.space/lsass.exe	2%	Virustotal		Browse
http://https://intergalacticaeronautic.space/lsass.exe	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://intergalacticaeronautic.space/win32.exe	0%	Avira URL Cloud	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://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://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
intergalacticaeronautic.space	91.195.240.13	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://login.microsoftonline.com/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://shell.suite.office.com:1443	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://cdn.entity.	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://wus2-000.contentsync.	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://powerlift.acompli.net	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Copyright null 2020

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://rpsticket.partnerservices.getmicrosoftkey.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://cortana.ai	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://api.aadrm.com/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://api.microsoftstream.com/api/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://cr.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://graph.ppe.windows.net	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://store.office.cn/addinstemplate	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://intergalacticaeronautic.space/lsass.exe	vbaProject.bin	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://web.microsoftstream.com/video/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://graph.windows.net	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://dataservice.o365filtering.com/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://intergalacticaeronautic.space/win32.exe	vbaProject.bin	false	• Avira URL Cloud: safe	unknown
http://https://prod-global-autodetect.acompli.net/autodetect	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://weather.service.msn.com/data.aspx	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://apis.live.net/v5.0/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.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	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://management.azure.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://outlook.office365.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://incidents.diagnostics.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://api.office.net	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://entitlement.diagnostics.office.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://autodiscover-s.outlook.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://templatelogging.office.com/client/log	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://management.azure.com/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://ncus-000.contentsync.	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://devnull.onenote.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://messaging.office.com/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://augloop.office.com/v2	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://skyapi.live.net/Activity/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://dataservice.o365filtering.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://directory.services.	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high
http://https://onedrive.live.com/embed?	458AAC77-423C-4DE6-AACC-E97569CD2F47.0.dr	false		high

Contacted IPs

Copyright null 2020



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.240.13	unknown	Germany		47846	SEDO-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321436
Start date:	22.11.2020
Start time:	05:57:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	acceptable_use_policy.docm
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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.winDOCM@1/8@1/1

Copyright null 2020

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docm
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, WinStore.App.exe, RuntimeBroker.exe, Microsoft.Photos.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, UsoClient.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe, Defrag.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 52.147.198.201, 52.109.32.27, 52.109.88.39, 52.109.12.23, 51.104.144.132, 2.20.84.85, 20.54.26.129, 67.26.137.254, 67.26.83.254, 8.248.119.254, 8.241.11.126, 8.248.113.254, 51.104.139.180, 92.122.213.194, 92.122.213.247, 52.155.217.156, 2.20.85.126, 40.126.1.130, 40.126.1.145, 20.190.129.160, 40.126.1.128, 20.190.129.24, 20.190.129.133, 20.190.129.17, 40.126.1.166, 93.184.220.29, 51.124.78.146, 40.127.240.158 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.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, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, www.tm.a.prd.aadg.akadns.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, settingsfd-prod-weu1-endpoint.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.13	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• www.smobz.com/ukj/?Ezu=6QwYUCSLPFcKJYuBdUDYqHrTALkpF8bqM6rRklucBz4KsP3ogUDK0i/zbdTcuU1sFZfY&lhuL6=Txol_LV
	#Uc720#Ud2f0#Uc544#Uc774#Ud14c#Ud06c-#Ubc1c#Uc8fc#Uc11c #Uc1a1#Ubd80#Uc758#Uac74.exe	Get hash	malicious	Browse	• www.smobz.com/ukj/?BZ=6QwYUCSLPFcKJYuBdUDYqHrTALkpF8bqM6rRkIucBz4KsP3ogUDK0i/zbdT2xkFsBbXY&l48=4hOl78_
	nel.exe	Get hash	malicious	Browse	• www.officee421.com/ns424/?KzrPX=kzrxP8&lJEpgpp=Cbpn9HPdnDvxKwh9tZDgvWZ3FWN5DdzTd5Eh64pT0MIinpxEBbCqVi4obr5cHTy4QQ+KEGF/dw==
	168768566-104646-sdfnt5-8.exe	Get hash	malicious	Browse	• www.app7924.com/sr1/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
intergalacticaeronautic.space	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEDO-ASDE	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• 91.195.241.137
	new file.exe.exe	Get hash	malicious	Browse	• 91.195.241.136
	Bonifico n.1101202910070714.exe	Get hash	malicious	Browse	• 91.195.241.136
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 91.195.241.136
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 91.195.241.136
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136
	http://ww1.0ffice.com/	Get hash	malicious	Browse	• 91.195.240.14
	New Additional Agreement.exe	Get hash	malicious	Browse	• 91.195.240.94
	UBEH7JEUC0.exe	Get hash	malicious	Browse	• 91.195.241.136
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• 91.195.240.13
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	ORDER7098EAR.exe	Get hash	malicious	Browse	• 91.195.241.136
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• 91.195.240.94
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136

Copyright null 2020

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	http://https://elharless.github.io/stamapdevmo/tak.html?bbre=oadfis48sd	Get hash	malicious	Browse	• 91.195.240.13
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 91.195.240.13
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 91.195.240.13
	http://https://flyboyfurnishings.com/firstam/RD-FITT	Get hash	malicious	Browse	• 91.195.240.13
	http://webnavigator.co	Get hash	malicious	Browse	• 91.195.240.13
	http://www.947947.mirramodaintima.com.br/#aHR0cHM6Ly9lbXl0dXJrLmNvbS9zZC9JSy9vZjEvRmlkZWwuVG9ycmVzQHNlYXJzaGMuY29t	Get hash	malicious	Browse	• 91.195.240.13
	http://microsoftonlineofficeteam.weebly.com	Get hash	malicious	Browse	• 91.195.240.13
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	http://rwiqipwvnklaqkuu.ltiliqhting.com/asci/SmFjcXVlbGluZS5TY2hyYWRlckByYWJvYmFuay5jb20=	Get hash	malicious	Browse	• 91.195.240.13
	Payment conflict- aptiv 082920134110.htm	Get hash	malicious	Browse	• 91.195.240.13
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 91.195.240.13
	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLIXyaU89Q?e=Ee0wW2	Get hash	malicious	Browse	• 91.195.240.13
	http://https://coralcliffs.com.do/review/	Get hash	malicious	Browse	• 91.195.240.13
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 91.195.240.13
	http://https://hastebin.com/raw/xatuvoxixa	Get hash	malicious	Browse	• 91.195.240.13
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 91.195.240.13
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 91.195.240.13
	Purchase Order Updates thyssenkrupp Materials Australia 900-5400006911.exe	Get hash	malicious	Browse	• 91.195.240.13

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\458AAC77-423C-4DE6-AACC-E97569CD2F47	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	129952
Entropy (8bit):	5.378329902349823
Encrypted:	false
SSDEEP:	1536:DcQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:BmQ9DQW+zBX8u
MD5:	5DEC13940FA582C3EA0D14686F3674FD
SHA1:	C10EC028EA4BE0192DED9B2257E2507E43AC2AA1
SHA-256:	A4443A4BE9754BEFBCA0FCC06404E2FCBB509295FCE466E46F11207D1A8C63F5
SHA-512:	87F34A3F48641BAA84A152A944CD46E8B1525A367B48FADB630000A15263E8F904CFFE49FD0C2BA8C37804EF7BA2B2DFFE78DB1C071B625C3BD02FCB47C0ED95
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\458AAC77-423C-4DE6-AACC-E97569CD2F47	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2020-11-22T04:58:02">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9B25BFFB-6D12-46BF-B5B1-512850D872C8}.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\Content.Word\~WRS{FD09A822-1B2C-450C-8498-115819ECFCCF}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	39472
Entropy (8bit):	4.066495003231631
Encrypted:	false
SSDEEP:	768:+gXnxdZBHbJ5rhVgkABKEuzs3ouLORZkFzj6ShJ7VHzwNgNRIhfYXZBFQg/rV:TcZVB
MD5:	9937792D604A0FE2C681ADD5873A0864
SHA1:	AE878B6731904130E4D00911C66E33A09D258D4A
SHA-256:	FEC7B469671CD5FCE86870C34D8DE4D8BEDB8B17551F5864B15C429FC9EB380C
SHA-512:	2309D50F95EAD1BD388EA07F5480403E6F07BB24F93DB63EFF826BA3E0472E10E42EA925956AC17665F090E92EE11AC06E0A8CDD60098DD6A77B5012E81C7C3
Malicious:	false
Reputation:	low
Preview:	..... .!.".#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....A.c.c.e.p.t.a.b.l.e. .U.s.e. .P.o.l.i.c.y.....O.v.e.r.v.i.e.w...I.n.f.o.s.e.c..s. .i.n.t.e.n.t.i.o.n.s. .f.o.r. .p.u.b.l.i.s.h.i.n.g. .a.n. .A.c.c.e.p.t.a.b.l.e. .U.s.e. .P.o.l.i.c.y. .a.r.e. .n.o.t. .t.o. .i.m.p.o.s.e. .r.e.s.t.r.i.c.t.i.o.n.s. .t.h.a.t. .a.r.e. .c.o.n.t.r.a.r.y. .t.o. .I.n.t.e.r.g.a.l.a.c.t.i.c. .A.e.r.o.n.a.u.t.i.c.s.. s..... .....d.....^.....d.....^.....d.....,]...^.....&..F.....E.....`..... .....^.....^.....$...K...<...[.].K.^.<.a

C:\Users\user\AppData\Local\Temp\mso71A1.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87841
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'.;..b...RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8....>.....4567...=..../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\acceptable_use_policy.docm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:41 2020, mtime=Sun Nov 22 12:58:02 2020, atime=Sun Nov 22 12:58:00 2020, length=765751, window=hide
Category:	dropped
Size (bytes):	2230
Entropy (8bit):	4.711827176004228
Encrypted:	false
SSDEEP:	24:8SjliNAyw39MQAKGmn9MmDg7/7aB6mySjliNAyw39MQAKGmn9MmDg7/7aB6m:8nfyMnKG0M3+B6pnfyMnKG0M3+B6
MD5:	89875041F76B2E458B839CF7C278EDC7
SHA1:	1CBE26C3919B5EA2CC49118D6B67E946BB677210
SHA-256:	0A4C41597E28B200FDCEFF05A40926752E05DFA7C153DB0E2A78E4477A31F14F
SHA-512:	2B7F3BC3E87212117C7E5FAC8505B4C81C300F01E5575F3F8948522D0160099AAFB59D66B2EB464D489621562E6FFA1B530B255458796DCA9BC2DFD607F04EB6
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....c.:...-K.~.....9}....7.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..vQ7o.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qvx..user.<.....Ny.vQ7o.....S.....f.h.a.r.d.z.....~.1.....>Qwx..Desktop.h.....Ny.vQ7o.....Y.....>.....R.i.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....2.7...vQAo .ACCEPT~1.DOC..f.....>QuxvQAo....h.....V...a.c.c.e.p.t.a.b.l.e._.u.s.e._.p.o.l.i.c.y...d.o.c.m.....`.....-....._.....>.S.....C:\Users\user\Desktop\acceptable_use_policy.docm..1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.c.c.e.p.t.a.b.l.e._.u.s.e._.p.o.l.i.c.y...d.o.c.m.....:..,.LB.)...As...`.....X.....528110.....!a..%.H.VZAj...U..-.....-..!a..%.H.VZAj...U..-.....-.....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.

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):	118
Entropy (8bit):	4.471727614263811
Encrypted:	false
SSDEEP:	3:HPRwcMMEG2prScGFcMMEG2prSmxWPRwcMMEG2prSv:HPRsRGO4RGOeRsRGOI
MD5:	F294413B5F2DEC815C4B94797368F7E5
SHA1:	D5008F974E54419BCD734905DBD3FCE2B01D56BD
SHA-256:	D3FCAE6B0458FF86847E03DF46CFEAABAA51DAB99F0640FE70B31DCD2B43EFEE
SHA-512:	803EA26E5435C15C1E0A7BC11FF977B4D2D3CEB4A5F934C6FE6273F85AFAB4223A58ECDAB88E4E6DA6AF05BCA361AB0D67B9FA57CC972BA782BB324EF53E4166
Malicious:	false
Reputation:	low
Preview:	[misc]..acceptable_use_policy.docm.LNK=0..acceptable_use_policy.docm.LNK=0..[misc]..acceptable_use_policy.docm.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):	1.9627417684431894
Encrypted:	false
SSDEEP:	3:Rl/Zdz7U/7LM6llXtlT7ElXR/f:RtZxQXTlpU
MD5:	343F68A09B6EA740190C49FF52AF2A8F
SHA1:	4945114B4BB0414850755367A067E204FF134425
SHA-256:	7922B26341B03E2668AB107124FE26BB6E6AE1783B101A56D09DA740BE3D6998
SHA-512:	7AA1B48C15F1739A43FAF1C9B618EFFA816E0D22FC029C413A26ACFCE7A9B95DF2A1FA1A1B912EA1ADE7855300CFD6F3A7709BC9EFF22FD4111E70ACC2DC74EA
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....q@.....M@.....I@.....H...

C:\Users\user\Desktop\~$ceptable_use_policy.docm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.9627417684431894
Encrypted:	false
SSDEEP:	3:Rl/Zdz7U/7LM6llXtlT7ElXR/f:RtZxQXTlpU
MD5:	343F68A09B6EA740190C49FF52AF2A8F
SHA1:	4945114B4BB0414850755367A067E204FF134425

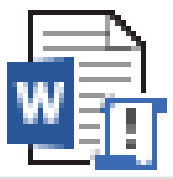
C:\Users\user\Desktop\~$ceptable_use_policy.docm	
SHA-256:	7922B26341B03E2668AB107124FE26BB6E6AE1783B101A56D09DA740BE3D6998
SHA-512:	7AA1B48C15F1739A43FAF1C9B618EFFA816E0D22FC029C413A26ACFCE7A9B95DF2A1FA1A1B912EA1ADE7855300CFD6F3A7709BC9EFF22FD4111E70ACC2DC74EA
Malicious:	false
Reputation:	low
Preview:	.pratesh...p.r.a.t.e.s.h...........q@.............................M@.............................I@............H...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.974352084549378
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:	acceptable_use_policy.docm
File size:	785211
MD5:	d651d3331b60eeeb49eb0fdc17b7b1df
SHA1:	bb816e1502b0baaa77742fde8c25bbc42c717674
SHA256:	a0a9eca457bd72df44a7ff398b5b4469bb4d1057fd43d7906c948b99f7be51ca
SHA512:	48ab987baa051f3c95c205ff3c65f0f77389f92a74791e44195c655c4e84523112ac9e060a31679994c47e6677c7f7bde6d84521684ed3cdee86c1df16270ed6
SSDEEP:	12288:Jnw0QEKpz/X0Ud46KsXhbSPhSxIxTqwwptJ22/baZ2J/SBxgegx:JwUKpzMn6LB5xmTqwwLc2FSBi5x
File Content Preview:	PK..........!.?9..............[Content_Types].xml ...(...

File Icon



Icon Hash:	74fcd0d2f692908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/321436/sample/acceptable_use_policy.docm"

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

Title:	
Subject:	

Copyright null 2020

Summary	
Author:	Glenn
Keywords:	
Template:	Normal
Last Saved By:	Glenn
Revion Number:	10
Total Edit Time:	7
Create Time:	2019-10-23T16:40:00Z
Last Saved Time:	2020-06-04T00:49:00Z
Number of Pages:	7
Number of Words:	1990
Number of Characters:	11349
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	94
Number of Paragraphs:	26
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: 3038

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	3038
Data ASCII:	. . . . b . . . . M . . . . < . . . . . . > I M + # $ M . G . . H . . . . y . . . . $ @ . . + . 6 = ... q 2 . P . H K . . . . / + 8 . . . . x . . . . q 2 . P . . H K . . . . / + 8 . . > I M + # $ M . G . . H . . . . M E . . . .
Data Raw:	01 16 01 00 04 00 01 00 00 16 06 00 00 e4 00 00 00 62 02 00 00 92 06 00 00 a0 06 00 00 d8 09 00 00 00 00 00 00 01 00 00 00 4d 9e bb bb 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 3c 00 ff ff 00 00 c3 3e 49 4d 2b 23 24 4d ad 47 8a 0d 48 a3 bf 9c 2e 79 0d df 0e bd 24 40 b7 c5 2b ee 36 3d 86 fd 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Shell(l,
o.Close
o.Write
VB_Name
VB_Creatable
VB_Exposed
r.Status
ActiveDocument.Path
"GET",
o.SaveToFile
CreateObject("Microsoft.XMLHTTP")
String
Object
o.Type
CreateObject("ADODB.Stream")
VB_Customizable
r.send
o.Open
"https://intergalacticaeronautic.space/lsass.exe"
Document_Open()
r.Open
VB_TemplateDerived

Keyword
"ThisDocument"
False
"\lsass.exe"
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
r.responseBody

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 366

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	366
Entropy:	5.32151305526
Base64 Encoded:	True
Data ASCII:	I D = " { 4 5 8 7 1 3 E 5 - 7 7 D A - 4 E C 6 - 9 0 7 7 - 0 1 1 A C 2 4 A 7 C 1 9 } " . . 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 . . 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 = " B 9 B B 0 6 7 E 0 A 7 E 0 A 7 E 0 A 7 E 0 A " . . D P B = " 7 2 7 0 C D 9 6 8 7 9 7 8 7 9 7 8 7 " . . G C = " 2 B 2 9 9 4 5 1 4 C 5 2 4 C 5 2 B 3 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0
Data Raw:	49 44 3d 22 7b 34 35 38 37 31 33 45 35 2d 37 37 44 41 2d 34 45 43 36 2d 39 30 37 37 2d 30 31 31 41 43 32 34 41 37 43 31 39 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 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2765

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2765
Entropy:	4.23158328116
Base64 Encoded:	False
Data ASCII:	. a . . . . . , . * . \ \ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \ \ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \ \ . 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 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 09 0c 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 2c 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 30 00 2d 00 43 00 30 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: 1752

General	
Stream Path:	VBA/__SRP_0
File Type:	data

General	
Stream Size:	1752
Entropy:	4.25450094175
Base64 Encoded:	False
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ b . . . . H . . . . . . N . . . x | . . k . . . . E . . . . y . . . .
Data Raw:	93 4b 2a af 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 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 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 102

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	102
Entropy:	2.15571505385
Base64 Encoded:	False
Data ASCII:	r U . . . . ~ } . . . . 1 . . . . p . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 7d 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 03 00 00 09 f9 02 00 00 00 00 00 00 31 06 00 00 00 00 00 00 08 00 00 00 00 00 01 00 70 00 00 7f 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 796

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	796
Entropy:	3.84331960003
Base64 Encoded:	False
Data ASCII:	r U . . . . 0 . . . . a . . . . I . . . . A . . . . A . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 01 00 01 00 14 00 00 00 c1 06 00 00 00 00 00 00 61 0a 00 00 00 00 00 00 e1 07 00 00 00 00 00 00 b9 07 00 00 00 00 00 00 91 05 00 00 00 00 00 00 09 08 00 00 00 00 00 00 a1 08 00 00 00 00 00 00 49 08 00 00 00 00 00 00 99 0a 00 00 00 00

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

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	2.08761800893
Base64 Encoded:	False
Data ASCII:	r U . . . . @ . . . . . $ . . . . ` . . . . n . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 40 00 00 00 04 00 24 00 01 01 00 00 00 00 02 00 00 00 04 60 00 00 00 07 1c 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: VBA/dir, File Type: shared library, Stream Size: 520

General	
Stream Path:	VBA/dir
File Type:	shared library
Stream Size:	520
Entropy:	6.28781093451
Base64 Encoded:	True

Copyright null 2020

General	
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . t . ` . . . . 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 04 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 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 d4 74 c4 60 06 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



Total Packets: 64

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 05:58:03.724476099 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.745862961 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.745954037 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.746823072 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.768229008 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.781511068 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.781553984 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.781642914 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.781704903 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.781769037 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.781815052 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.781847000 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.800757885 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.822292089 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.822618008 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.822741985 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.823468924 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:03.845011950 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.846674919 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:03.846795082 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:58:33.844568968 CET	443	49720	91.195.240.13	192.168.2.3
Nov 22, 2020 05:58:33.844810963 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:59:52.325941086 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:59:52.636311054 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:59:53.245578051 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:59:54.449029922 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 05:59:56.855210066 CET	49720	443	192.168.2.3	91.195.240.13
Nov 22, 2020 06:00:01.668390036 CET	49720	443	192.168.2.3	91.195.240.13

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:00:11.278481960 CET	49720	443	192.168.2.3	91.195.240.13

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 05:57:56.514345884 CET	63492	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:57:56.550137997 CET	53	63492	8.8.8.8	192.168.2.3
Nov 22, 2020 05:57:57.549412966 CET	60831	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:57:57.576673985 CET	53	60831	8.8.8.8	192.168.2.3
Nov 22, 2020 05:57:58.655307055 CET	60100	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:57:58.682600975 CET	53	60100	8.8.8.8	192.168.2.3
Nov 22, 2020 05:57:59.377094030 CET	53195	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:57:59.404274940 CET	53	53195	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:00.512104988 CET	50141	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:00.539453030 CET	53	50141	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:01.735061884 CET	53023	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:01.770982981 CET	53	53023	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:02.401407957 CET	49563	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:02.440853119 CET	53	49563	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:02.918054104 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:02.966746092 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:03.622884035 CET	59349	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:03.650130033 CET	53	59349	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:03.675304890 CET	57084	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:03.722489119 CET	53	57084	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:03.932637930 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:03.968533993 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:04.555044889 CET	58823	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:04.582184076 CET	53	58823	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:04.924555063 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:04.964778900 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:05.210623026 CET	57568	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:05.246499062 CET	53	57568	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:06.323802948 CET	50540	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:06.351104021 CET	53	50540	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:06.940100908 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:06.977041960 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:07.374743938 CET	54366	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:07.401978016 CET	53	54366	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:08.450762033 CET	53034	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:08.486824036 CET	53	53034	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:10.940638065 CET	51352	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:10.978610039 CET	53	51352	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:22.630690098 CET	57762	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:22.658009052 CET	53	57762	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:31.029139042 CET	55435	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:31.068272114 CET	53	55435	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:34.403594017 CET	50713	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:34.447336912 CET	53	50713	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:47.110378981 CET	56132	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:47.137634993 CET	53	56132	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:56.385293961 CET	58987	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:56.412652969 CET	53	58987	8.8.8.8	192.168.2.3
Nov 22, 2020 05:58:59.186183929 CET	56579	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:58:59.223818064 CET	53	56579	8.8.8.8	192.168.2.3
Nov 22, 2020 05:59:30.982765913 CET	60633	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:59:31.009998083 CET	53	60633	8.8.8.8	192.168.2.3
Nov 22, 2020 05:59:32.174042940 CET	61292	53	192.168.2.3	8.8.8.8
Nov 22, 2020 05:59:32.209918976 CET	53	61292	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:46.765994072 CET	63619	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:46.806549072 CET	53	63619	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:47.310528040 CET	64938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:47.352988958 CET	53	64938	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:47.828701019 CET	61946	53	192.168.2.3	8.8.8.8

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:00:47.866602898 CET	53	61946	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:48.156594038 CET	64910	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:48.192480087 CET	53	64910	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:48.537071943 CET	52123	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:48.573080063 CET	53	52123	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:49.338268042 CET	56130	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:49.373930931 CET	53	56130	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:50.457032919 CET	56338	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:50.492697954 CET	53	56338	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:53.260564089 CET	59420	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:53.296427011 CET	53	59420	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:54.470021009 CET	58784	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:54.506095886 CET	53	58784	8.8.8.8	192.168.2.3
Nov 22, 2020 06:00:54.926553965 CET	63978	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:00:54.964607954 CET	53	63978	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:20.572392941 CET	62938	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:20.624505997 CET	53	62938	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:46.046202898 CET	55708	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:46.113405943 CET	53	55708	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:46.219773054 CET	56803	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:46.247029066 CET	53	56803	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:46.581609964 CET	57145	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:46.625842094 CET	53	57145	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:47.210067987 CET	55359	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:47.260608912 CET	53	55359	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:47.642524958 CET	58306	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:47.669866085 CET	53	58306	8.8.8.8	192.168.2.3
Nov 22, 2020 06:02:47.802000046 CET	64124	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:02:47.839972973 CET	53	64124	8.8.8.8	192.168.2.3
Nov 22, 2020 06:05:01.915260077 CET	49361	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:05:01.942634106 CET	53	49361	8.8.8.8	192.168.2.3
Nov 22, 2020 06:05:34.531680107 CET	63150	53	192.168.2.3	8.8.8.8
Nov 22, 2020 06:05:34.558928967 CET	53	63150	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 05:58:03.675304890 CET	192.168.2.3	8.8.8.8	0x5ee	Standard query (0)	intergalacticaeronautic.space	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 05:58:03.722489119 CET	8.8.8.8	192.168.2.3	0x5ee	No error (0)	intergalacticaeronautic.space		91.195.240.13	A (IP address)	IN (0x0001)
Nov 22, 2020 06:02:46.113405943 CET	8.8.8.8	192.168.2.3	0xa74	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 05:58:03.781704903 CET	91.195.240.13	443	192.168.2.3	49720	CN=intergalacticaeronautic.space CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 29 02:00:00 CEST 2020 Mon Nov 27 13:46:10 CET 2017 Fri Nov 10 01:00:00 CET 2006	Wed Jun 30 14:00:00 CEST 2021 Sat Nov 27 13:46:10 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 27 13:46:10 CET 2017	Sat Nov 27 13:46:10 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 5360 Parent PID: 792

General

Start time:	05:58:01
Start date:	22/11/2020
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x1190000
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	66B8977C	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66ADD539	unknown

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	66AC8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	66AC8A84	RegCreateKeyExA

Copyright null 2020

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly