ID: 320290
Sample Name: doc2227740.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:54:17
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

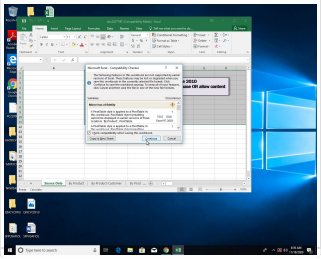
Analysis Report doc2227740.xls

Overview

General Information

Sample Name:	doc2227740.xls
Analysis ID:	320290
MD5:	b43d8b40f9ef159..
SHA1:	3c0d89ac4b439b..
SHA256:	196588a7404c90..
Tags:	xls ZLoader

Most interesting Screenshot:



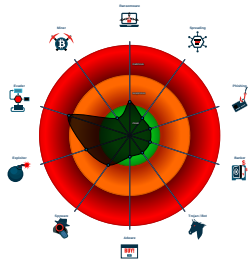
Detection

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Found Excel 4.0 Macro with suspicio…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…
- Queries the volume information (nam…
- Tries to load missing DLLs
- Yara detected Xls With Macro 4.0
- Yara signature match

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 4092 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - MSOSYNC.EXE (PID: 2916 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe MD5: EA19F4A0D18162BE3A0C8DAD249ADE8C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

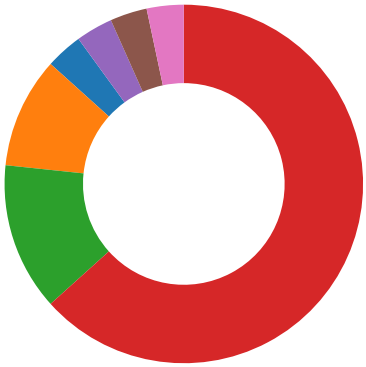
Initial Sample

Source	Rule	Description	Author	Strings
doc2227740.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0xbf4b:$s1: Excel • 0xfc43:$s1: Excel • 0x10187:$s1: Excel • 0x11376:$s1: Excel • 0x1574d:$s1: Excel • 0x157aa:$s1: Excel • 0x157cd:$s1: Excel • 0x38c6:$Auto_Close: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 00 02 3A
doc2227740.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Software Vulnerabilities
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

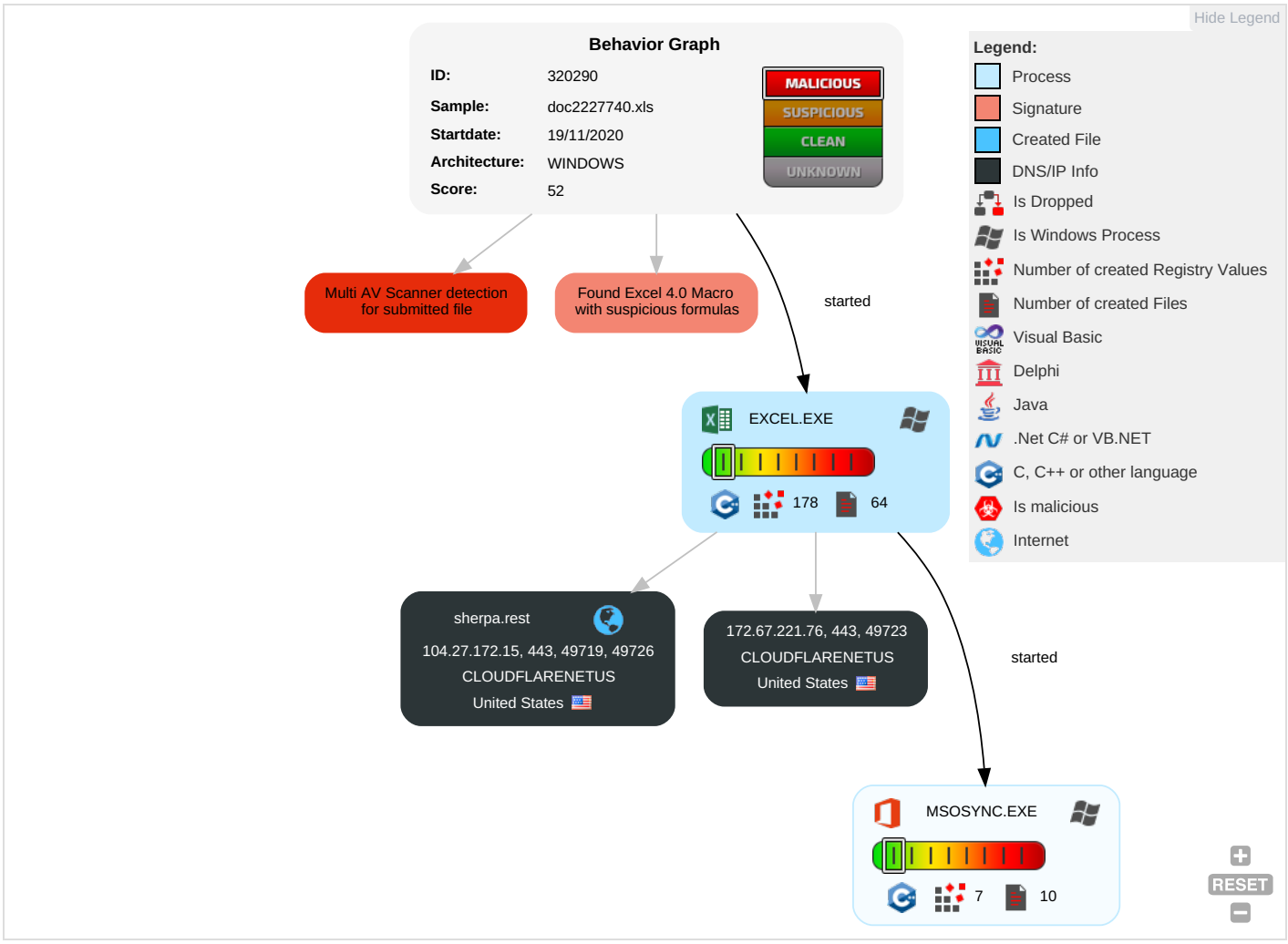
System Summary:

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	I
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	
Default Accounts	Exploitation for Client Execution 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	System Information Discovery 1 1	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	
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1	Security Account Manager	Remote System Discovery 1	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	
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		

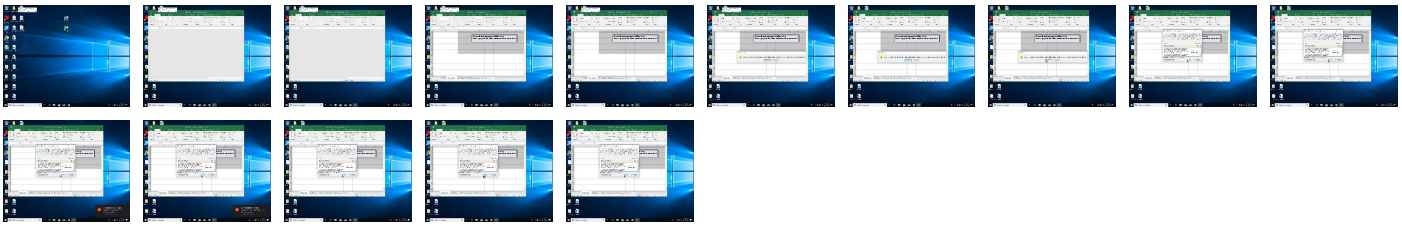
Behavior Graph

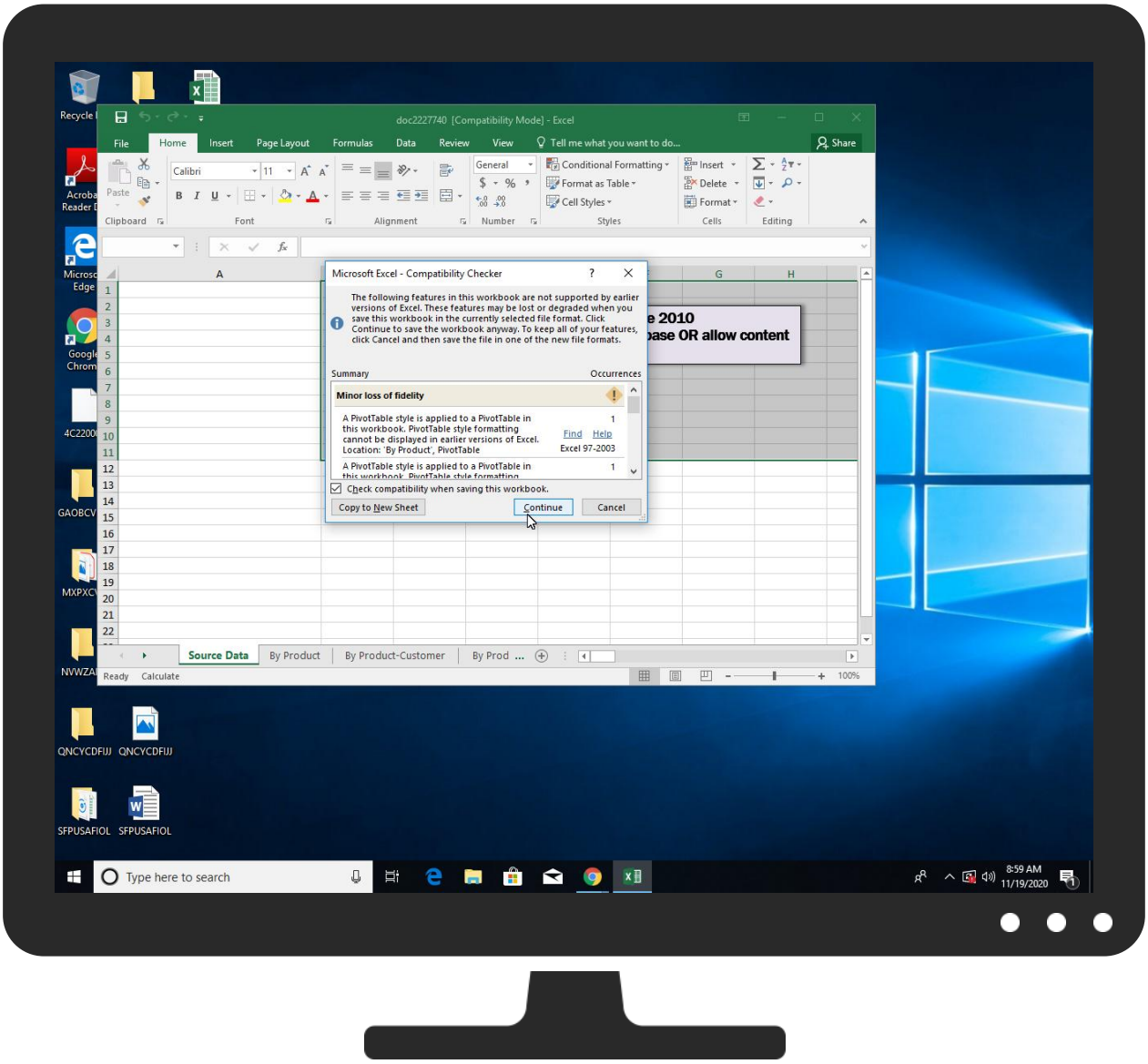


Screenshots

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
doc2227740.xls	21%	ReversingLabs	Document-Excel.Dropper.SDrop	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sherpa.rest	0%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
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-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-user.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	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	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://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%	Virustotal		Browse
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://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://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://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://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
sherpa.rest	104.27.172.15	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

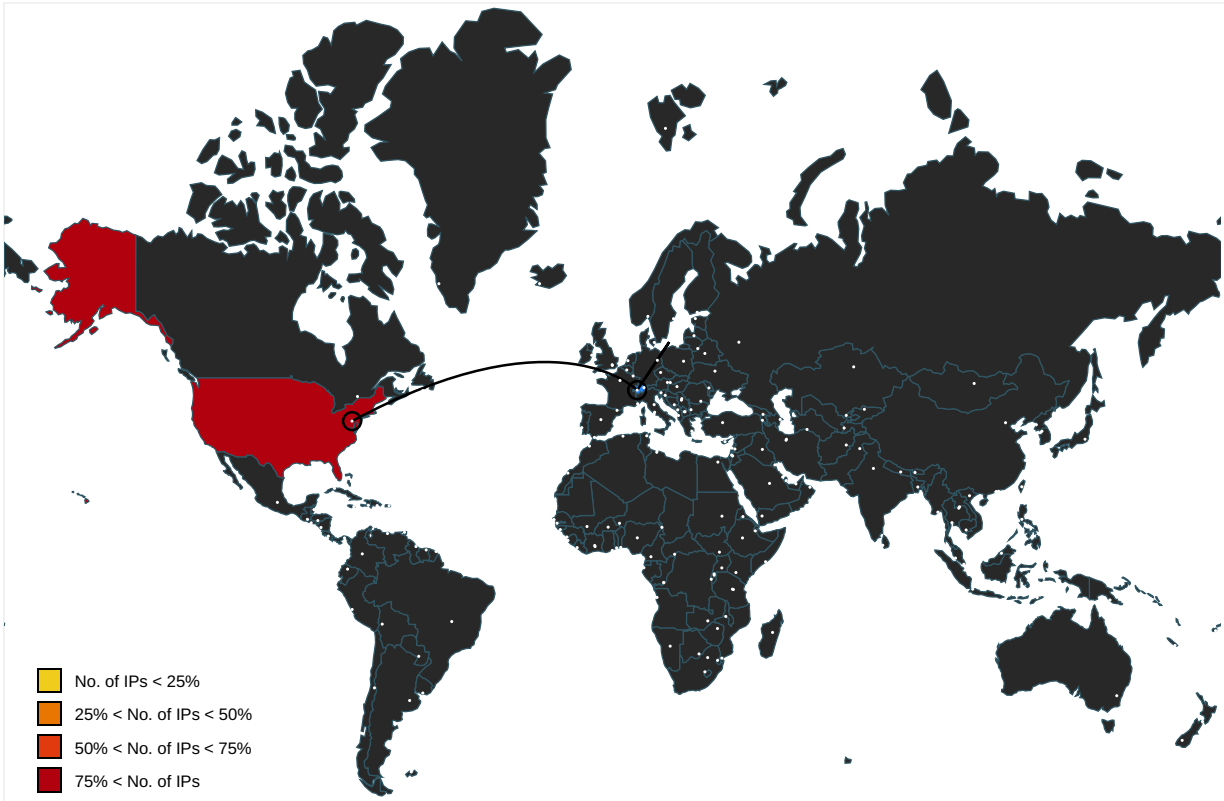
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://login.microsoftonline.com/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://shell.suite.office.com:1443	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://cdn.entity.	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://wus2-000.contentsync.	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.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	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://cortana.ai	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.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	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://api.aadrm.com/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://api.microsoftstream.com/api/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://cr.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://graph.ppe.windows.net	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-user.acompli.net	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://store.office.cn/addinstemplate	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.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=	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://web.microsoftstream.com/video/	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://graph.windows.net	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://dataservice.o365filtering.com/	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://weather.service.msn.com/data.aspx	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://apis.live.net/v5.0/	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.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	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://management.azure.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://outlook.office365.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://incidents.diagnostics.office.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://api.office.net	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	617A6017-3014-4CF5-A8EA-F75B71 4BAAF0.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://entitlement.diagnostics.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://autodiscover-s.outlook.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://templatelogging.office.com/client/log	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://management.azure.com/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://ncus-000.contentsync.	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://devnull.onenote.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://messaging.office.com/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://augloop.office.com/v2	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://skyapi.live.net/Activity/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://dataservice.o365filtering.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://directory.services.	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows-ppe.net/common/oauth2/authorize	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://loki.delve.office.com/api/v1/configuration/officewin32/	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://onedrive.live.com/embed?	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://augloop.office.com	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high
http://https://www.bingapis.com/api/v7/urlpreview/search?appid=E93048236FE27D972F67C5AF722136866DF65FA2	617A6017-3014-4CF5-A8EA-F75B714BAAF0.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.221.76	unknown	United States		13335	CLOUDFLARENETUS	false
104.27.172.15	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320290
Start date:	19.11.2020
Start time:	08:54:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc2227740.xls
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:	36
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:	mal52.evad.winXLS@3/10@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to English - United States
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): MpCmdRun.exe, WinStore.App.exe, RuntimeBroker.exe, backgroundTaskHost.exe, ApplicationFrameHost.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, MusNotifyIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 52.109.88.8, 52.109.12.21, 52.109.88.39, 40.88.32.150, 23.54.113.104, 51.104.144.132, 13.88.21.125, 23.0.174.185, 23.0.174.200, 51.103.5.159, 52.155.217.156, 52.147.198.201, 20.54.26.129, 23.10.249.26, 23.10.249.43, 51.11.168.160, 13.104.215.69, 13.104.215.72, 40.90.23.154, 40.90.23.208, 40.90.23.206, 40.90.137.124, 40.90.137.126, 40.90.23.153, 93.184.220.29, 40.127.240.158, 20.49.150.241, 23.54.113.45 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, fs-wildcard.microsoft.com.edgekey.net, wns.notify.windows.com.akadns.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, login.live.com, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, europe.configsvc1.live.com.akadns.net, www.tm.lg.prod.aadmsa.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, prod-w.nexus.live.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, par02p.wns.notify.windows.com.akadns.net, blu-main-ips-v4only.a.lg.prod.aadmsa.trafficmanager.net, emea1.notify.windows.com.akadns.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, prod.configsvc1.live.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, settings-win.data.microsoft.com, a767.dscg3.akamai.net, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, config.officeapps.live.com, settingsfd-prod-neu1-endpoint.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtReadVirtualMemory 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
172.67.221.76	d11311145.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sherpa.rest	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.13 4.233
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66
	e2b97ee03b4b38578f04d0cc93d8effd.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://app.archbee.io/doc/wjFBJ1IQgNqcYtxyaUfi5/V9dqJTS3iO58EgXIT7wr1	Get hash	malicious	Browse	• 104.17.234.61
	http://https://msgcash.com/click/NzhlMWY1MTltNzg3NS00ZDFmLTk1YmQtODZiZGQ3MzQwZGMz	Get hash	malicious	Browse	• 172.67.181.196
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://Https://christinescom.github.io/cappdevs/ta.html?bbre=dsiw4risd	Get hash	malicious	Browse	• 104.16.19.94
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	• 104.17.201.204
	http://https://lfonoumkgl.zizera.com/FX	Get hash	malicious	Browse	• 104.16.18.94
CLOUDFLARENETUS	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.13 4.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	07DYwxlVm4.exe	Get hash	malicious	Browse	• 104.27.133.115
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 162.159.133.233
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 172.67.38.66
	e2b97ee03b4b38578f04d0cc93d8effd.exe	Get hash	malicious	Browse	• 104.27.133.115
	http://https://app.archbee.io/doc/wjFBJ1IQgNqcYtxyaUfi5/V9dqJTS3iO58EgXIT7wr1	Get hash	malicious	Browse	• 104.17.234.61
	http://https://msgcash.com/click/NzhlMWY1MTltNzg3NS00ZDFmLTk1YmQtODZiZGQ3MzQwZGMz	Get hash	malicious	Browse	• 172.67.181.196
	bGtm3bQKUj.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://Https://christinescom.github.io/cappdevs/ta.html?bbre=dsiw4risd	Get hash	malicious	Browse	• 104.16.19.94
	http://https://olhonabrasa.com.br/secure/zimbra/access/zimbra/index.php	Get hash	malicious	Browse	• 104.17.201.204
	http://https://lfonoumkgl.zizera.com/FX	Get hash	malicious	Browse	• 104.16.18.94

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	d11311145.xls	Get hash	malicious	Browse	• 104.27.172.15
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.172.15
	af4db3a6b648b585f8e11b9ff5be73f2.exe	Get hash	malicious	Browse	• 104.27.172.15
	WSGaRIW.dll	Get hash	malicious	Browse	• 104.27.172.15
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 104.27.172.15
	ddos_____ (IW0Irt2zSey6D6LMEgcs2kqQiSuMa 8 G).js	Get hash	malicious	Browse	• 104.27.172.15
	e2b97ee03b4b38578f04d0cc93d8effd.exe	Get hash	malicious	Browse	• 104.27.172.15
	MIT-MULTA5600415258.msi	Get hash	malicious	Browse	• 104.27.172.15
	Q4Esp4M8dM.msi	Get hash	malicious	Browse	• 104.27.172.15
	WOHSFR01BZAC6VP3YOYSGIHL92J4B0XM50RJR34.dll	Get hash	malicious	Browse	• 104.27.172.15
	#U007e370531.dll	Get hash	malicious	Browse	• 104.27.172.15
	WSGaRIW.dll	Get hash	malicious	Browse	• 104.27.172.15
	ad2b6de5fb2ee29b62d3a71195beffd1.exe	Get hash	malicious	Browse	• 104.27.172.15
	C51sYmlcZU.dll	Get hash	malicious	Browse	• 104.27.172.15
	MhgKT501bC.exe	Get hash	malicious	Browse	• 104.27.172.15
	SecuriteInfo.com.Trojan.PWS.Siggen2.59718.4609.exe	Get hash	malicious	Browse	• 104.27.172.15
	45g7l63ZII.exe	Get hash	malicious	Browse	• 104.27.172.15
	qTgBzp3G6n.exe	Get hash	malicious	Browse	• 104.27.172.15
	35xLEdpG78.exe	Get hash	malicious	Browse	• 104.27.172.15
	start.exe	Get hash	malicious	Browse	• 104.27.172.15
37f463bf4616ecd445d4a1937da06e19	d11311145.xls	Get hash	malicious	Browse	• 172.67.221.76
	Original Shipment Document.exe	Get hash	malicious	Browse	• 172.67.221.76
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 172.67.221.76
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 172.67.221.76
	http://www.ericbess.com/ericblog/2008/03/03/wp-codebox/#examples	Get hash	malicious	Browse	• 172.67.221.76
	http://https://app.archbee.io/doc/wjFBJ1IQgNqcYtxyaUfi5/V9dqJTS3iO58EgXIT7wr1	Get hash	malicious	Browse	• 172.67.221.76
	http://https://lfonoumkgl.zizera.com/FX	Get hash	malicious	Browse	• 172.67.221.76
	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 172.67.221.76
	http://https://view.publitas.com/ipinsurance/demers-beaulne-inc/	Get hash	malicious	Browse	• 172.67.221.76
	ACH - WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 172.67.221.76
	http://https://t.co/DmCKxDTz1S	Get hash	malicious	Browse	• 172.67.221.76
	http://customer.cartech.com/inventory_manufacturing.cfm	Get hash	malicious	Browse	• 172.67.221.76
	ACHWIRE REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 172.67.221.76
	http://https://www.canva.com/design/DAEN4Gk1aAs/uErgK6sn3gPozGMXWtYgqA/view?utm_content=DAEN4Gk1aAs&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 172.67.221.76

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	win_encryptor.exe	Get hash	malicious	Browse	• 172.67.221.76
	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	• 172.67.221.76
	http://https://www.google.com/url?q=https://sedgefuneralplan.com/pinafore.php&sa=D&ust=1605725146740000&usg=AOvVaw1JCRUh1siinDaulCG91nF3	Get hash	malicious	Browse	• 172.67.221.76
	http://https://bxjg2oj292.zizera.com/F00929377	Get hash	malicious	Browse	• 172.67.221.76
	ACH & WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 172.67.221.76

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.accdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	626709
Entropy (8bit):	0.5031071884738996
Encrypted:	false
SSDEEP:	384:5IJC48SFq/fZ0jGB5bQYLWtwtZ1IV+hVZO4FAvWGTHi5hF:6C4HEZLUht/2iTH+X
MD5:	F76279857E6EEF0A400CDC66D4481273
SHA1:	904A4D8EE1639003E636BD434F066B33308654AF
SHA-256:	FE4F12EB6414CAC4845EF34C6FBF5A3FFC6C1ADD51C56E2FB5D058F90361A03B
SHA-512:	E66A8B40BEB1DDDB11A28D832B66096C9817486003D6F29FABC9391FEFB5B9BA313FF36243DA28A8D23CE1476466B96E3F391964617ED2CB7C73233867A2E47
Malicious:	false
Reputation:	low
Preview:	.....Standard ACE DB.....n.b`..U.gr@?..~.....1.y..0...c...F...N.W.7'....(.i..`.8{6....X.C...3N.y[..|*..|.....YS/q'..f_...$.g..'D...e....F.x....-b.T...4.0..... ....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.ini

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	36
Entropy (8bit):	2.730660070105504
Encrypted:	false
SSDEEP:	3:5NixJlElGUR:WrEcUR
MD5:	1F830B53CA33A1207A86CE43177016FA
SHA1:	BDF230E1F33AFBA5C9D5A039986C6505E8B09665
SHA-256:	EAF9CDC741596275E106DDDCF8ABA61240368A8C7B0B58B08F74450D162337EF
SHA-512:	502248E893FCFB179A50863D7AC1866B5A466C9D5781499EBC1D02DF4F6D3E07B9E99E0812E747D76734274BD605DAD6535178D6CE06F08F1A02AB60335DE06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	C.e.n.t.r.a.l.T.a.b.l.e...a.c.c.d.b.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
File Type:	data
Category:	modified
Size (bytes):	64
Entropy (8bit):	1.4172860556164644
Encrypted:	false
SSDEEP:	3:B//FFaV:p/Hu
MD5:	E698F24BC9310DEFAFA33DC18788A7FD
SHA1:	68B43654690AA4ABF0E5EE8D878240FF9FA8F588
SHA-256:	488C20172E44B59D6D2A3B25E5059E4EDEF39282A7960E325CA99D0596B4524E
SHA-512:	5A7D53C9592E8B78B8C7E06D71C84FFFCE0A8279D0E6C4BF9E50ACA8D66410FAA176A788EF675D71B13AA3BEF871E9293D501A01FE302CD3AF522129BF4EB79

C:\Users\user\AppData\Local\Microsoft\Office\16.0\OfficeFileCache\CentralTable.laccdb	
Malicious:	false
Reputation:	low
Preview:	216041. Admin.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\617A6017-3014-4CF5-A8EA-F75B714BAAF0	
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):	129952
Entropy (8bit):	5.378350056332974
Encrypted:	false
SSDEEP:	1536:+cQceNWiA3gZwLpQ9DQW+zAUH34ZldpKWXboOilXPErLL8TT:cmQ9DQW+zBX8u
MD5:	128DBF8C46E8139662B35A0CC4157738
SHA1:	FE6D65207AC0671A57A6EE362D89BBDC7EECF2CB
SHA-256:	776598D04D9B6E6F0E19C0C2D63E73475D1EDB99239FA1AFA884C4CB8897A0DD
SHA-512:	4326161E7CB3D3407EBE2E1B9BFDA8FF5B2C326B29FED16B20772F585DBB759108B1CB8EE3962F4068EBE085B1718CEF4A5BC65DE10C4CF36CACC18D286C9A 58
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="2020-11-19T07:55:16">.. Build: 16.0.13517.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\ED120000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	47395
Entropy (8bit):	7.751135057057903
Encrypted:	false
SSDEEP:	768:8VuhzHYkZ6Z0xeyLkcTcNvL0h4utZss/aEf/WBQ/e4py+vz:8VuhEkZ6tcTcNvIh4utZsSaO/WCWh+vz
MD5:	A6236930282FAC3FC1646B9C0AB4B3D1
SHA1:	E22EA64D9D73EADC161443708813185836D0CC6B
SHA-256:	BEBB34F7015B6B46347DC152FBE96B03A4BCF38D36598545D9CBD07CAF3ADFD6
SHA-512:	04AC96CB4A9C250B095E292915F2B364BC27057D7D2FA0B815EF4C407CB9144A627536976F8A44C1AD7900F629B6BB7FC3C8BB6A72D7BAE8ABBB0639F66063D 9
Malicious:	false
Reputation:	low
Preview:	.V..!.}OU.a.....T*...<&[Y....Cd....O..&..qV..2.2}.ih..Z.X.....=R..V*3._.o.gR.....r5|..?^9..F.0 U...cATP.@...3S.k..1...].z...&..eL.d...S~.cq...J&.b...Q..wN+.#.e.#.#).t..H+.j.. .y.2T....y....b...a...t.F..bd..*..;L}.C...&..n.W.....w^c.l....sz.$-M.JX..4.Ok...6\|...2...0..sh`.u.s..B.....oe...-~G..Gd..:....^.../....#.....Q...s8..K.GK.7*...z..N..E[.+.X~..%.....\+k.6.{.../..... .Cz~.$....u...S..t..l..')...(9.....=^....r..bT..8.l....b.o...".v...f....,Y.&.....]@..{r...E....G.[Sw..-.....K...,{.....PK.....!.-|.$.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	170164
Entropy (8bit):	4.363228647751794
Encrypted:	false
SSDEEP:	1536:fLMKLfolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:fVc8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	585D4D9F489465C7910F738F54015231
SHA1:	8D7DDBDD54965DB24B8DB697D2847402AAA38401
SHA-256:	01D994455C78DACD432531EED4FF112C0E860C5B7B1A70774C9D2059065BAA14
SHA-512:	7304543BBFCDC591C77BFE8F91852B5E324049067233FFCA0112691EE1D50B52D3B0210F85A907CF670EA5FE984F4700978DFE3CAE1E090E9C35C6355287D76F
Malicious:	false
Reputation:	low
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.....$..... .....x...l.....T..... ....

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 19:05:17 2019, mtime=Thu Nov 19 15:55:42 2020, atime=Thu Nov 19 15:55:42 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	920
Entropy (8bit):	4.682108861205002
Encrypted:	false
SSDEEP:	12:8ECDU9peCHqDGqgkXe/6AEeM8+WMEjAt/rbD7b1e0b1eZ44t2Y+xIBjKZm:8EOVglLNMxQAtvDuw7aB6m
MD5:	0616211745B3EB0F248AE7A299558A42
SHA1:	E9496DE0593D39EEFC0C21B76F15493F6B78C5D7
SHA-256:	E789AF734829983C00D4210911915144074ABB97CCD20B54F202B63D8663ACA2
SHA-512:	AA61E1470D056BDB2A04AA90EACBE224D5AC843E0BE30C08D0DAE992F7CE8F0E95B0723FB7C3D145BCC654528583627BB1E5029E8033C685613367F91EEB50 3
Malicious:	false
Reputation:	low
Preview:	L.....F.....)...#-...N..... .....P.O. .:i.....+00.../C:\.....x.1.....N...Users.d.....L..sQ.....:.....1.U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1 .3.....\.1.....>Q.{..user~1..D.....N..sQ.....S.....a.f.r.o.n.t.d.e.s.k.....~.1.....sQ....Desktop.h.....N..sQ.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7 .6.9.....I.....-.....H.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\D.e.s.k.t.o.p.....:..,.LB.)...A....`.....X.....216041.....!a..%.H.VZAj...8T..... .....!a..%.H.VZAj...8T.....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...1S PS..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):	26
Entropy (8bit):	4.315824333525707
Encrypted:	false
SSDEEP:	3:bDesBVov:bSsjy
MD5:	1063941D0DFB4EEF54E229F8824BBF78
SHA1:	F5D426DD401DEF6D899B39A724A2CBD49B5E723C
SHA-256:	1F5532486F511ECE84285BB578119EF28A15A44E4E63DC63C92F2EAEA5D7A25D
SHA-512:	82DAA6F61F7FB49FA88660101915700B66F2B4E285559B8381902239922D83FFAD76C970D25FCEEC4C2E716733453789575B76A52E5C75CDF4A277F71770B696
Malicious:	false
Reputation:	low
Preview:	[folders]..Desktop.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Wed Nov 18 06:47:39 2020, Security: 0

General

Entropy (8bit):	4.360697246981449
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	doc2227740.xls
File size:	88576
MD5:	b43d8b40f9ef15965d0ff901e30c2f32
SHA1:	3c0d89ac4b439b7cf60b6cc6e4195a8ce3514572
SHA256:	196588a7404c90ab92502926afa24fbb25bf67c0ad50dba4f7ff4f1937816dda
SHA512:	57e42961b4ffe2b4233e05e8619a4dd59a9f00a7c68bf4cc57843cb6f3803c51c727287d9407c4787b5fb8be2caff1105e30abd4c82c9ccc3b335ff9e754c72e
SSDEEP:	1536:C3xEtjPOtioVjDGUU1qfDlaGGx+cL2QnAUA4duNxABg/geJtJSuAO1arCFsi:C3xEtjPOtioVjDGUU1qfDlaGGx+cL2QD
File Content Preview:	.....>.....P..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "doc2227740.xls"

Indicators

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

Summary

Code Page:	1251
Author:	
Keywords:	
Last Saved By:	
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2020-11-18 06:47:39
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Category:	PmFbdwr0TuP
Thumbnail Scaling Desired:	False
Manager:	
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False

Document Summary	
Application Version:	983040

Streams with VBA

VBA File Name: Sheet1.cls, Stream Size: 5844

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	5844
Data ASCII:	. . . . 8 . . . . I : . . . . # . . . . < . . . . b R 3 N M . f I . . . . F . . . . # I . A . . X N . . . V . . . . x . . . . # I . A . . X N . . . V . . . b R 3 N M . f I . . . . M E . . . .
Data Raw:	01 16 01 00 03 00 01 00 00 cc 05 00 00 e4 00 00 00 38 02 00 00 fb 05 00 00 09 06 00 00 85 10 00 00 00 00 00 00 01 00 00 00 a7 f5 6c 3a 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 3c 00 ff ff 00 00 d1 cf 0f 62 52 33 4e 4d 98 66 49 f6 90 cb a7 dd 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
BackgroundQuery:=False
TEXTJOIN(Delimiter
.AdjustColumnWidth
True,
(Len(x)
seconds)
.WebConsecutiveDelimitersAsOne
Public
.WebFormatting
Resume
Mid(TEXTJOIN,
"Range"
ActiveSheet.QueryTables.Add(Connection:=
While
.WorkbookConnection.Delete
False
Wait(seconds
"htt"
www.TheSpreadsheetGuru.com
xlInsertDeleteCells
MakeWebQuery
String,
Cell.Value
Excel
"lol"
String
MakeWebQuery()
Len(RangeArea)
Len(Cell.Value)
.Refresh
Destination:=
.WebSelectionType
VB_GlobalNameSpace
shFirstQtr
Range
.FillAdjacentFormulas
"ps:"
.PreserveFormatting
.BackgroundQuery
"info.p"
.WebDisableDateRecognition
Through
RangeArea
VB_Base

Keyword
Boolean,
.WebSingleBlockTextImport
.PostText
Given
VB_Creatable
VB_Exposed
Input
Entered
Integer)
VB_TemplateDerived
Empty
(Timer
Ignore_Empty
.WebPreFormattedTextToColumns
ParamArray
.SavePassword
'SOURCE:
"info"
Worksheet_Activate()
Error
.WebDisableRedirections
Attribute
'PURPOSE:
VB_PredeclaredId
Timer()
VB_Name
Private
TypeName(RangeArea)
CONCAT
"//sherpa"
Function
Variant
xlWebFormattingNone
Len(Delimiter)
VB_Customizable
".rest/wp-"
"pic"
DoEvents
'.RefreshStyle
xlEntirePage
swedr
'Text
"URL;"
Delimiter
.RefreshOnFileOpen
.RowNumbers
'Loop
Variant)
Replicates
Worksheet_Calculate()
TEXTJOIN
.RefreshPeriod
TEXTJOIN("",

VBA Code

VBA File Name: Sheet2.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet2
VBA File Name:	Sheet2.cls
Stream Size:	977

General	
Data ASCII:	. . . . \\ [. . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 a7 f5 5c 5b 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Sheet3.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet3
VBA File Name:	Sheet3.cls
Stream Size:	977
Data ASCII:	. . . . q . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 a7 f5 bd 71 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Sheet4.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet4
VBA File Name:	Sheet4.cls
Stream Size:	977
Data ASCII:	. . . . c . . . . . # . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 a7 f5 63 fc 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Sheet5.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet5
VBA File Name:	Sheet5.cls
Stream Size:	977
Data ASCII:	. . . . . - b . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 a7 f5 2d 62 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 985

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	985
Data ASCII:	. . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 a7 f5 ab 7f 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: UserForm1.frm, Stream Size: 2834

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	2834
Data ASCII:	. . . . . 0 . . . . . t . . . . . 8 . . . . . ^ R . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 01 f0 00 00 00 30 04 00 00 d4 00 00 00 74 02 00 00 ff ff ff ff 38 04 00 00 e0 07 00 00 00 00 00 01 00 00 00 a7 f5 5e 52 00 00 ff ff 01 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
#FileNumber
requirement
Close
Error
VB_Name
VB_Creatable
/one"
VB_Exposed
xFileName
Print
FileNumber
Empty
String
Resume
Variant
Output
"c:\Users\Public"
VB_Customizable
#FileNumber,
":jsoncronipont
Replace("wsconroniponton
"\Documents\"
Range
Dir(Path)
Integer
DelimChar
VB_TemplateDerived
False
ThisWorkbook.BuiltinDocumentProperties("Keywords")
Attribute
Debug.Print

Keyword
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
'Change
FreeFile
strFileExists

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 107

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	107
Entropy:	4.18482950044
Base64 Encoded:	True
Data ASCII:	. . . . F . . . . M i c r o s o f t E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 1f 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 424

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	424
Entropy:	3.70704949759
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . x . . . . . ` . . . . . h . . . . . | . . . . . 2 . . . . . P m F b d w r 0 T u P . . . . . S o u r c e D
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 78 01 00 00 0b 00 00 00 01 00 00 00 60 00 00 00 02 00 00 00 68 00 00 00 0e 00 00 00 7c 00 00 00 0f 00 00 00 88 00 00 00 17 00 00 00 94 00 00 00 0b 00 00 00 9c 00 00 00 10 00 00 00 a4 00 00 00 13 00 00 00 ac 00 00 00 16 00 00 00 b4 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 220

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	220
Entropy:	3.13229188015
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . H . . . . . P . . . . . \\ . . . . . h . . . . . t . . . . . M i c r o s o f t E x c e l . @ . . . . . | . # . . . @ . . . . . v . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 ac 00 00 00 08 00 00 00 01 00 00 00 48 00 00 00 04 00 00 00 50 00 00 00 05 00 00 00 5c 00 00 00 08 00 00 00 68 00 00 00 12 00 00 00 74 00 00 00 0c 00 00 00 8c 00 00 00 0d 00 00 00 98 00 00 00 13 00 00 00 a4 00 00 00 02 00 00 00 e3 04 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 39260

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	39260
Entropy:	4.61059933587

General	
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... i . . 9 J . 8
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 c0 01 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _SX_DB_CUR/0001, File Type: data, Stream Size: 16815

General	
Stream Path:	_SX_DB_CUR/0001
File Type:	data
Stream Size:	16815
Entropy:	2.76744715124
Base64 Encoded:	True
Data ASCII:	. . . . A u t h o r " . . . E # . . . . . @ . . . . P r d u c t . . . . A l i c e M u t t o n . . . . A n i s e e d S y r u p . . . . B o s t o n C r a b M e a t . . . . C a m e m b e r t P i e r r o t . . . . C h e f A n t o n ' s C a j u n S e a s o n i n g . . . . C h e f A n t o n ' s G u m b o M i x . . . . F i l o M i x . . . . G o r
Data Raw:	c6 00 1b 00 15 01 00 00 01 00 03 00 1c 07 06 00 06 00 00 00 01 00 06 00 00 41 75 74 68 6f 72 22 01 0c 00 45 23 01 9f f7 fc e2 40 00 00 00 00 c7 00 18 00 81 14 00 00 00 00 19 00 00 00 00 00 19 00 07 00 00 50 72 6f 64 75 63 74 bb 01 02 00 00 00 cd 00 0f 00 0c 00 00 41 6c 69 63 65 20 4d 75 74 74 6f 6e cd 00 10 00 0d 00 00 41 6e 69 73 65 65 64 20 53 79 72 75 70 cd 00 13 00 10 00 00 42

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 826

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	826
Entropy:	5.15315553776
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 2 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 3 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 4 / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 5 / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 32 2f 26 48 30 30 30

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 176

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	176
Entropy:	3.18343768922
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . S h e e t 2 . S . h . e . e . t . 2 . . . S h e e t 3 . S . h . e . e . t . 3 . . . S h e e t 4 . S . h . e . e . t . 4 . . . S h e e t 5 . S . h . e . e . t . 5 . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 53 68 65 65 74 32 00 53 00 68 00 65 00 65 00 74 00 32 00 00 00 53 68 65 65 74 33 00 53 00 68 00 65 00 65 00 74 00 33 00 00 00 53 68 65 65 74 34 00 53 00 68 00 65 00 65 00 74 00 34 00 00 00 53 68 65 65 74

Stream Path: _VBA_PROJECT_CUR/UserForm1/\x1CompObj, File Type: data, Stream Size: 97

General	
Stream Path:	_VBA_PROJECT_CUR/UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306

General	
Base64 Encoded:	False
Data ASCII:	. . . . . Microsoft Forms 2.0 Form . . . . . Embedded Object . . . . . 9.q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 291

General	
Stream Path:	_VBA_PROJECT_CUR/UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	291
Entropy:	4.60170100243
Base64 Encoded:	True
Data ASCII:	VERSION 5.00 . . Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 . . Caption = "UserForm1" . . ClientHeight = 3165 . . ClientLeft = 45 . . ClientTop = 390 . . ClientWidth = 4710 . . StartUpPosition = 1 'CenterOwn
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: _VBA_PROJECT_CUR/UserForm1/f, File Type: data, Stream Size: 171

General	
Stream Path:	_VBA_PROJECT_CUR/UserForm1/f
File Type:	data
Stream Size:	171
Entropy:	3.84288648278
Base64 Encoded:	False
Data ASCII:	. . $ . . . . . } . . t . . . . . R . . . . . K . Q . . . . . D B . . . Tahoma . . . . . X . . . . . $ . . . . . 4 . . . . . TextBox1O . . . . . (. . . . . 2 . . . 8 . . . . . Label1 . . " . . . { . . .
Data Raw:	00 04 24 00 08 0c 10 0c 02 00 00 00 ff ff 00 00 02 00 00 00 00 7d 00 00 74 20 00 00 cf 15 00 00 00 00 00 00 00 00 00 03 52 e3 0b 91 8f ce 11 9d e3 00 aa 00 4b b8 51 01 cc 00 00 90 01 44 42 01 00 06 54 61 68 6f 6d 61 00 00 02 00 00 00 58 00 00 00 00 82 01 00 00 00 24 00 e5 01 00 00 08 00 00 80 01 00 00 00 34 00 00 00 00 00 17 00 54 65 78 74 42 6f 78 31 4f 03 00 00 ca 05 00 00 00

Stream Path: _VBA_PROJECT_CUR/UserForm1/o, File Type: data, Stream Size: 108

General	
Stream Path:	_VBA_PROJECT_CUR/UserForm1/o
File Type:	data
Stream Size:	108
Entropy:	3.31418568251
Base64 Encoded:	False
Data ASCII:	. . . . . H . . . . . ; . . . . . 5 . . . . . Tahoma . . . . . (. . . . . Label1 . . . . . { . . . . . 5 . . . . . Tahoma . .
Data Raw:	00 02 14 00 01 01 00 80 00 00 00 00 1b 48 00 ac ce 18 00 00 3b 0a 00 00 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00 cc 02 00 00 54 61 68 6f 6d 61 00 00 00 02 18 00 28 00 00 00 06 00 00 80 4c 61 62 65 6c 31 00 00 ec 09 00 00 7b 02 00 00 00 02 18 00 35 00 00 00 06 00 00 80 a5 00 00 00 cc 02 00 00 54 61 68 6f 6d 61 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4896

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4896
Entropy:	4.8370296249
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 . . (. x . 8 . 6 .) . \\ . 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 . . .

General	
Data Raw:	cc 61 a3 00 00 01 00 ff 00 20 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 2c 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 2d 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_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1828

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	1828
Entropy:	4.3476580333
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ h . . . . . % . . . . 9] H . . 8 . . . . .
Data Raw:	93 4b 2a a3 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 01 00 02 00 01 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 68 00 00 7f

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 191

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	191
Entropy:	3.30829134406
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ } . . . . . s e c o n d s . . . . . D e l i m i e r . . . . . I g n o r e _ E m p t y . . . . . T e x t 1 a . . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 7d 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff 09 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 03 00 00 09 a1 03 00 00 00 00 00 00 81 08 00 00 00 00 00 00 08 00 00 00 00 00 01 00 02 00 00 08 07 00 00 00 73 65

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 384

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	384
Entropy:	2.45306416855
Base64 Encoded:	False
Data ASCII:	r U . . . . . 0 . . . . . Y . . . . . 4 . . . . . a . . . . . 0 . . . . . ` . . . . . ` . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 09 08 00 00 00 00 00 00 31 08 00 00 00 00 00 00 59 08 00 00 00 00 00 00 ff ff ff ff e1 07 00 00 00 00 00 00 08 00 18 00 34 00 00 00 81 08 00 00 00 00 00 00 61 00 00 00 00 00 01 00 a9 08

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 294

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	294
Entropy:	2.65487119554
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . (. . . . . ` . . a . . . . . & 8 . A . . . . . ` . . e . . . . . 0 # o . . 0 $ . . . . . ` . . i . . . . . $ . . . . . ` . . . . . $ . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 40 00 00 00 04 00 28 00 01 01 00 00 00 00 02 00 00 00 03 60 04 00 61 02 ff ff ff ff ff ff ff ff 00 00 00 00 81 00 00 00 00 00 01 00 00 00 00 00 1e 26 38 00 41 01 00 00 00 00 02 00 01 00 03 60 10 fd 65 02 ff ff ff ff ff ff ff ff 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: MIPSEL-BE Ucode, Stream Size: 902

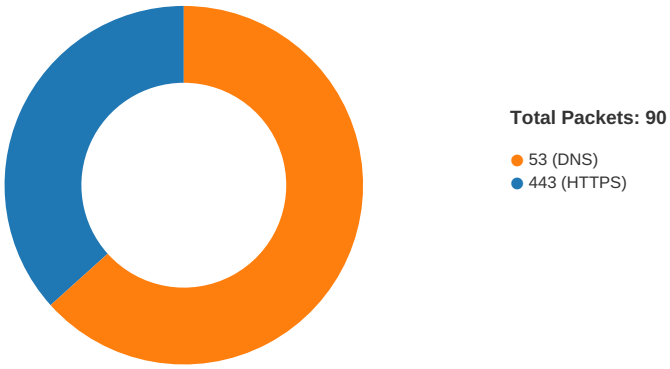
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	MIPSEL-BE Ucode
Stream Size:	902
Entropy:	6.58076213885
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . B . a . . . . . J < . . . . . r . s t d 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 W O W 6 4 \ \ . 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 82 b3 80 01 00 04 00 00 00 01 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 c2 42 a1 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

Macro 4.0 Code

```
"=RETURN(EXEC(GET.WORKBOOK(36,DOCUMENTS(1))))",,=1+1
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:55:19.848890066 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.878330946 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.878441095 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.879019976 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.908390045 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.911714077 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.911746025 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.911758900 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.911838055 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.918428898 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.947875977 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.947994947 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:19.951216936 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:19.980967045 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:21.978830099 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:21.978873968 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:21.979068041 CET	49719	443	192.168.2.7	104.27.172.15

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:55:21.979769945 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:22.009512901 CET	443	49719	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:22.009630919 CET	49719	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:22.035882950 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.065563917 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.065721989 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.068093061 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.099931955 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.100008011 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.100061893 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.100142002 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.100194931 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.119996071 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.149784088 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.149807930 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:22.150031090 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.151693106 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:22.181390047 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:25.212553978 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:25.212766886 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:25.222140074 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:25.251995087 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:25.252108097 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:25.252711058 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:25.282305956 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:25.286920071 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:25.311943054 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:25.313043118 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:25.341367006 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:25.342783928 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:28.228908062 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:28.228935957 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:28.229162931 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:28.229494095 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:28.231627941 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:28.260252953 CET	443	49726	104.27.172.15	192.168.2.7
Nov 19, 2020 08:55:28.260447979 CET	49726	443	192.168.2.7	104.27.172.15
Nov 19, 2020 08:55:28.261111975 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:31.245928049 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:31.246103048 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:31.274483919 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:31.304227114 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.263920069 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.263946056 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.263959885 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.263972044 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.263988018 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.264000893 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.264017105 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.264034986 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.264050007 CET	443	49723	172.67.221.76	192.168.2.7
Nov 19, 2020 08:55:34.264123917 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:34.264163971 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:34.267493010 CET	49723	443	192.168.2.7	172.67.221.76
Nov 19, 2020 08:55:34.267533064 CET	49723	443	192.168.2.7	172.67.221.76

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:55:03.690892935 CET	58717	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:03.703077078 CET	53	58717	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:04.503283978 CET	59762	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:04.516273975 CET	53	59762	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:13.827972889 CET	54329	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:55:13.840821028 CET	53	54329	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:15.054418087 CET	58052	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:15.067482948 CET	53	58052	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:16.108428955 CET	54008	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:16.128803968 CET	53	54008	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:16.396924973 CET	59451	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:16.412990093 CET	53	59451	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:16.706808090 CET	52914	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:16.720577955 CET	53	52914	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:17.414170980 CET	59451	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:17.427687883 CET	53	59451	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:18.378830910 CET	64569	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:18.391457081 CET	53	64569	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:18.429977894 CET	59451	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:18.443228006 CET	53	59451	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:19.315308094 CET	52816	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:19.328758955 CET	53	52816	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:19.811559916 CET	50781	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:19.847448111 CET	53	50781	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:20.372431040 CET	54230	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:20.386019945 CET	53	54230	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:20.441660881 CET	59451	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:20.455090046 CET	53	59451	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:20.661062956 CET	54911	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:20.673784971 CET	53	54911	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:21.364162922 CET	54230	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:21.377136946 CET	53	54230	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:22.002232075 CET	49958	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:22.031665087 CET	53	49958	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:22.379714966 CET	54230	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:22.393177032 CET	53	54230	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:22.810425997 CET	50860	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:22.828685045 CET	53	50860	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:23.053925037 CET	50452	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:23.066096067 CET	53	50452	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:24.380263090 CET	54230	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:24.393002033 CET	53	54230	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:24.442250013 CET	59451	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:24.455365896 CET	53	59451	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:28.395911932 CET	54230	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:28.408533096 CET	53	54230	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:31.556031942 CET	59730	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:31.568850040 CET	53	59730	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:37.624082088 CET	59310	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:37.637690067 CET	53	59310	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:41.137947083 CET	51919	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:41.151437044 CET	53	51919	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:42.451525927 CET	64296	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:42.463757992 CET	53	64296	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:43.444963932 CET	56680	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:43.459101915 CET	53	56680	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:45.399720907 CET	58820	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:45.412800074 CET	53	58820	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:46.884980917 CET	60983	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:46.898097992 CET	53	60983	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:53.072124958 CET	49247	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:53.090845108 CET	53	49247	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:53.560739040 CET	52286	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:53.573664904 CET	53	52286	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:55.765737057 CET	56064	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:55.779037952 CET	53	56064	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:56.226586103 CET	63744	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:56.239907026 CET	53	63744	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:56.349257946 CET	61457	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 08:55:56.362277031 CET	53	61457	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:56.701160908 CET	58367	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:56.721797943 CET	53	58367	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:57.046128035 CET	60599	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:57.059211016 CET	53	60599	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:57.128667116 CET	59571	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:57.141024113 CET	53	59571	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:57.522999048 CET	52689	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:57.535382032 CET	53	52689	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:57.718154907 CET	50290	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:57.745742083 CET	53	50290	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:57.947175026 CET	60427	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:57.960751057 CET	53	60427	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:58.415807962 CET	56209	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:58.428867102 CET	53	56209	8.8.8.8	192.168.2.7
Nov 19, 2020 08:55:59.124157906 CET	59582	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:55:59.137289047 CET	53	59582	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:00.187294006 CET	60949	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:00.200376987 CET	53	60949	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:00.803838015 CET	58542	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:00.816900015 CET	53	58542	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:03.864377022 CET	59179	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:03.884466887 CET	53	59179	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:32.229438066 CET	60927	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:32.263771057 CET	53	60927	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:34.892143011 CET	57854	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:34.904783964 CET	53	57854	8.8.8.8	192.168.2.7
Nov 19, 2020 08:56:54.737792969 CET	62026	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:56:54.750781059 CET	53	62026	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:49.896569967 CET	59453	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:49.909166098 CET	53	59453	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:50.216155052 CET	62468	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:50.228629112 CET	53	62468	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:50.648753881 CET	52563	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:50.674897909 CET	53	52563	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:54.137573957 CET	54721	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:54.171084881 CET	53	54721	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:57.826704979 CET	62826	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:57.853064060 CET	53	62826	8.8.8.8	192.168.2.7
Nov 19, 2020 08:59:58.106853962 CET	62046	53	192.168.2.7	8.8.8.8
Nov 19, 2020 08:59:58.120014906 CET	53	62046	8.8.8.8	192.168.2.7
Nov 19, 2020 09:00:14.674246073 CET	51223	53	192.168.2.7	8.8.8.8
Nov 19, 2020 09:00:14.722126007 CET	53	51223	8.8.8.8	192.168.2.7
Nov 19, 2020 09:01:57.797785044 CET	63908	53	192.168.2.7	8.8.8.8
Nov 19, 2020 09:01:57.810509920 CET	53	63908	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 08:55:19.811559916 CET	192.168.2.7	8.8.8.8	0xa688	Standard query (0)	sherpa.rest	A (IP address)	IN (0x0001)
Nov 19, 2020 08:55:22.002232075 CET	192.168.2.7	8.8.8.8	0x84a7	Standard query (0)	sherpa.rest	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 08:55:19.847448111 CET	8.8.8.8	192.168.2.7	0xa688	No error (0)	sherpa.rest		104.27.172.15	A (IP address)	IN (0x0001)
Nov 19, 2020 08:55:19.847448111 CET	8.8.8.8	192.168.2.7	0xa688	No error (0)	sherpa.rest		104.27.173.15	A (IP address)	IN (0x0001)
Nov 19, 2020 08:55:19.847448111 CET	8.8.8.8	192.168.2.7	0xa688	No error (0)	sherpa.rest		172.67.221.76	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 08:55:22.031665087 CET	8.8.8.8	192.168.2.7	0x84a7	No error (0)	sherpa.rest		172.67.221.76	A (IP address)	IN (0x0001)
Nov 19, 2020 08:55:22.031665087 CET	8.8.8.8	192.168.2.7	0x84a7	No error (0)	sherpa.rest		104.27.173.15	A (IP address)	IN (0x0001)
Nov 19, 2020 08:55:22.031665087 CET	8.8.8.8	192.168.2.7	0x84a7	No error (0)	sherpa.rest		104.27.172.15	A (IP address)	IN (0x0001)

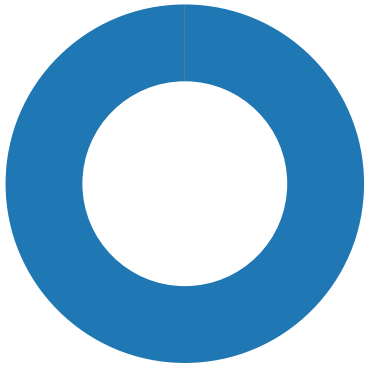
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 08:55:19.911746025 CET	104.27.172.15	443	192.168.2.7	49719	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Nov 01 01:00:00 CET 2020	Mon Nov 01 00:59:59 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Nov 19, 2020 08:55:22.100061893 CET	172.67.221.76	443	192.168.2.7	49723	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Sun Nov 01 01:00:00 CET 2020	Mon Nov 01 00:59:59 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 4092 Parent PID: 792

General

Start time:	08:55:15
Start date:	19/11/2020
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:	0xaf0000
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~1\AppData\Local\Temp\~DF2C3D4D1ED2C4ED54.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67F592AB	unknown
C:\Users\user~1\AppData\Local\Temp\~DF62673B03BF913B1D.TMP	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	67FAF261	unknown
C:\Users\user~1\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	6805977C	unknown
C:\Users\user~1\AppData\Local\Temp\VBE\MSForms.exd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67F93F8E	unknown
C:\Users\user\Application Data\Microsoft\Forms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	67F8E349	unknown
C:\Users\user\Application Data\Microsoft\Forms\EXCEL.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67F8E349	unknown
C:\Users\user~1\AppData\Local\Temp\~DF9811006287845619.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67F8E349	unknown
C:\Users\user~1\AppData\Local\Temp\~DF3AD4E4E853E6440B.TMP	read attributes | delete | syn chronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	67F8E349	unknown
C:\Users\user~1\AppData\Local\Temp\~DF9925737B8D03953D.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	680C7D31	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\~DF062BA3951E56271B.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6805703B	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\EXCEL.box	success or wait	1	67F8E349	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\EEDE8D98.tmp	success or wait	1	C6495B	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\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 6c 00 00 cc 42 00 00 0f 00 00 00	.....l...B......	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$...........	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0c 00 00 00 07 00 00 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 80 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 20 00 00 80 10 00 00 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 02 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 78 00 00 ec 49 00 00 0f 00 00 00	.....x...I......	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 20 00 00 00 10 00 00 00 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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 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 90 fd 94 0f 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 30 00 00 00 00 00 00 00 2c 00 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 70 13 95 0f 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 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,........................... ....p................. ....H.......D..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	38 10 00 00 f8 07 00 00 50 10 00 00 10 08 00 00 a8 0f 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 88 0b 00 00 20 10 00 00 58 0b 00 00 08 10 00 00 88 0e 00 00 68 10 00 00 d8 0f 00 00 88 05 00 00 48 0f 00 00 90 0c 00 00 10 0e 00 00 70 0e 00 00 78 0f 00 00 00 00 0f 00 00 30 0f 00 00	8.......P...........@......... ..X........................... (........... ...X...........h. ....H...........p...x.......0...	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	c5 ab 7a e1 07 e7 15 48 95 2f 2a cf 72 dd 86 af fe 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....H./*.r............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	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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 ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff 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 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 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 ff	....L........... ....p...h....... ....0..... ....d...............(# ....#............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	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 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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	28	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	...........-.stdole2.tlbWWW	success or wait	1	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	74 41 00 00 bc 24 00 00 5c 30 00 00 a8 49 00 00 e4 47 00 00 60 3c 00 00 f8 2d 00 00 58 45 00 00 2c 41 00 00 bc 47 00 00 88 30 00 00 cc 49 00 00 3c 2c 00 00 cc 48 00 00 70 46 00 00 68 3d 00 00 20 42 00 00 64 24 00 00 b8 3b 00 00 44 47 00 00 48 46 00 00 48 43 00 00 48 3e 00 00 94 26 00 00 4c 3c 00 00 18 3a 00 00 20 44 00 00 44 38 00 00 a8 45 00 00 18 47 00 00 80 45 00 00 10 43 00 00 14 49 00 00 84 49 00 00 2c 30 00 00 24 40 00 00 90 42 00 00 ac 44 00 00 1c 3e 00 00 ac 3f 00 00 34 42 00 00 14 45 00 00 98 47 00 00 a4 43 00 00 94 32 00 00 14 41 00 00 0c 48 00 00 5c 44 00 00 bc 45 00 00 84 28 00 00 c0 2f 00 00 ac 2d 00 00 e4 31 00 00 b4 41 00 00 b4 40 00 00 6c 34 00 00 e8 21 00 00 9c 40 00 00 40 3b 00 00 08 2a 00 00 6c 45 00 00 cc 40 00 00 24 46 00 00 fc 3e 00	tA...$..\0...I...G..`<...-..XE ..,A...G...0...I..<,...H..pF.. h=.. B..d$...;..DG..HF..HC..H> ...&..L<...:.. D..D8...E...G.. .E...C...I...I..,0..$@...B...D ...>...?..4B...E...G...C...2.. .A...H..\D...E...(.../...-...1 ...A...@..l4...!...@..@;...*.. lE...@..$F...>.	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18924	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	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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 L ibrary..C:\Windows\SysW OW64\fm 20.hlpWW..NoneWW..Cop yWW..Move WW..CopyOrMove..CutW WW..PasteW ..DragDropWW..InheritWW W..OnWW WW..OffWWW..DefaultW WW..ArrowW ..CrossW..IBeamW..SizeN ESWWW.. SizeNS..SizeNWSEWW..S izeWE..Up ArrowWWW..HourG	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	03 00 fe ff ff ff 57 57 03 00 ff ff ff ff 57 57	.....WW.....WW	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	.....L..D.....	success or wait	1757	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.....	success or wait	1215	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\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	....$...H...l..... ...D...h..... ....@...d.....	success or wait	107	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 5e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00	.^..............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	8c 67 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00	.g..............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	bc 57 00 00 00 07 00 00 ff ff ff ff 0f 00 00 00	.W..............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\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	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	3c 47 00 00 80 10 00 00 ff ff ff ff 0f 00 00 00	<G..............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	a8 67 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00	.g..............	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	a8 69 00 00 ec 49 00 00 ff ff ff ff 0f 00 00 00	.i...I..........	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	94 b3 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	e8 b9 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	f8 c7 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00	....	success or wait	1	67F93F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 08 c8 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 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 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 08 c8 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 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 08 c8 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 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....&!.................. ....0..... ..,........................... ....H.......D..	success or wait	1	67F93F8E	unknown

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	B620F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	B6211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67F98A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67F98A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67F98A84	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	B6213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	B6213B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1366491137	success or wait	1	67FF7FEE	unknown

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

Analysis Process: MSOSYNC.EXE PID: 2916 Parent PID: 4092

General

Start time:	08:55:19
Start date:	19/11/2020

Path:	C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\MsoSync.exe
Imagebase:	0xf40000
File size:	466688 bytes
MD5 hash:	EA19F4A0D18162BE3A0C8DAD249ADE8C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Disassembly