



ID: 403443
Sample Name: 9177284661-04302021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 05:55:45
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 9177284661-04302021.xlsm 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Initial Sample 4
Sigma Overview 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
Networking: 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 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static OLE Info 13
General 13
OLE File "/opt/package/joesandbox/database/analysis/403443/sample/9177284661-04302021.xlsm" 13
Indicators 13
Summary 14
Document Summary 14
Streams with VBA 14
VBA File Name: Byutut.bas, Stream Size: 1343 14
General 14
VBA Code Keywords 14
VBA Code 14
VBA File Name: Class1.cls, Stream Size: 999 14
General 14

Copyright Joe Security LLC 2021

VBA Code Keywords 14
VBA Code 15
Streams 15
Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 543 15
General 15
Stream Path: PROJECTwm, File Type: data, Stream Size: 107 15
General 15
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2831 15
General 15
Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 1642 15
General 15
Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 146 16
General 16
Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 170 16
General 16
Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 156 16
General 16
Stream Path: VBA/dir, File Type: data, Stream Size: 601 16
General 16
Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990 17
General 17
Stream Path: VBA/\x1051\x1080\x1089\x10902, File Type: data, Stream Size: 990 17
General 17
Stream Path: VBA/\x1069\x1090\x1072\x1050\x1085\x1080\x1075\x1072, File Type: data, Stream Size: 994 17
General 17
Macro 4.0 Code 17
Network Behavior 17
Snort IDS Alerts 18
TCP Packets 18
HTTP Request Dependency Graph 18
HTTP Packets 18
Code Manipulations 19
Statistics 19
System Behavior 20
Analysis Process: EXCEL.EXE PID: 2388 Parent PID: 584 20
General 20
File Activities 20
File Created 20
File Deleted 21
File Moved 21
File Written 21
File Read 27
Registry Activities 27
Key Created 27
Key Value Created 27
Disassembly 35

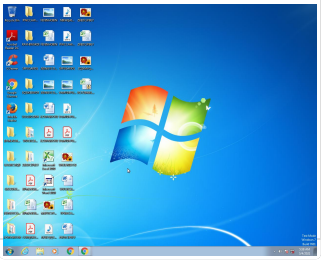
Analysis Report 9177284661-04302021.xlsm

Overview

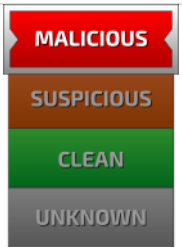
General Information

Sample Name:	9177284661-04302021.xlsm
Analysis ID:	403443
MD5:	a8b4e37766d35b..
SHA1:	4356c14118ea90..
SHA256:	533c8713c4e10c...
Infos:	

Most interesting Screenshot:



Detection



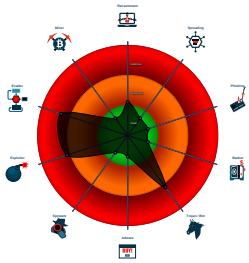
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for doma...
- Multi AV Scanner detection for subm...
- Document contains an embedded VB...
- Document exploit detected (UrlDown...
- Found Excel 4.0 Macro with suspicio...
- Yara detected MalDoc1
- Document contains an embedded VB...
- Document contains embedded VBA ...
- Potential document exploit detected...
- Potential document exploit detected...
- Uses a known web browser user age...

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2388 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

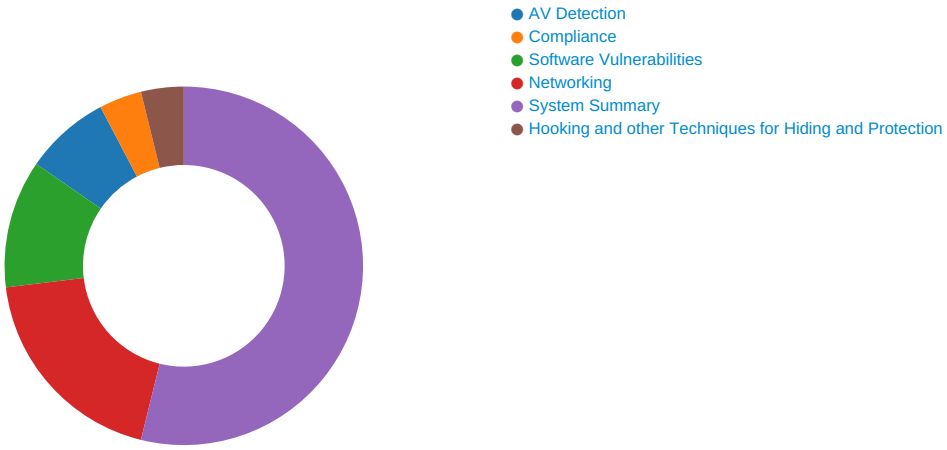
Source	Rule	Description	Author	Strings
sheet3.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Networking:

Yara detected MalDoc1

System Summary:

Found malicious Excel 4.0 Macro

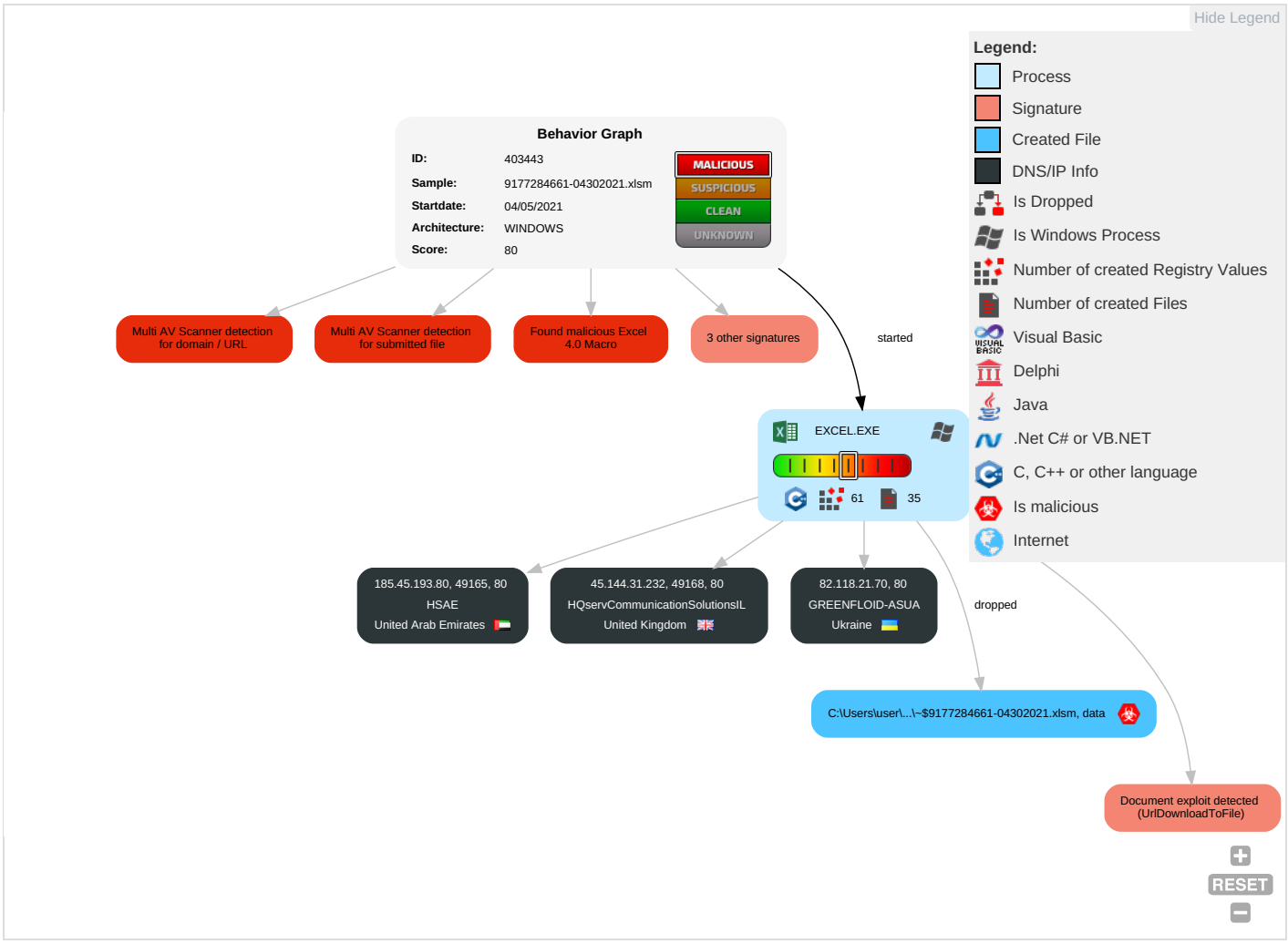
Document contains an embedded VBA macro which may execute processes

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

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

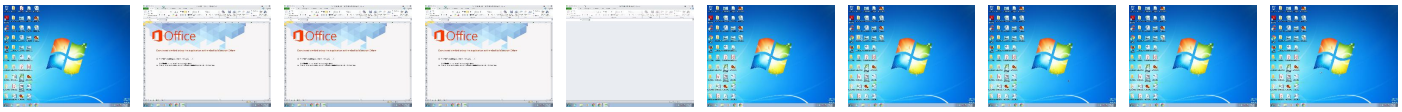
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
9177284661-04302021.xlsm	39%	Virustotal		Browse
9177284661-04302021.xlsm	32%	ReversingLabs	Document-Office.Trojan.Valyria	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.45.193.80/44313,6048108796.dat	7%	Virustotal		Browse
http://185.45.193.80/44313,6048108796.dat	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://45.144.31.232/44313,6048108796.dat	8%	Virustotal		Browse
http://45.144.31.232/44313,6048108796.dat	0%	Avira URL Cloud	safe	

Domains and IPs

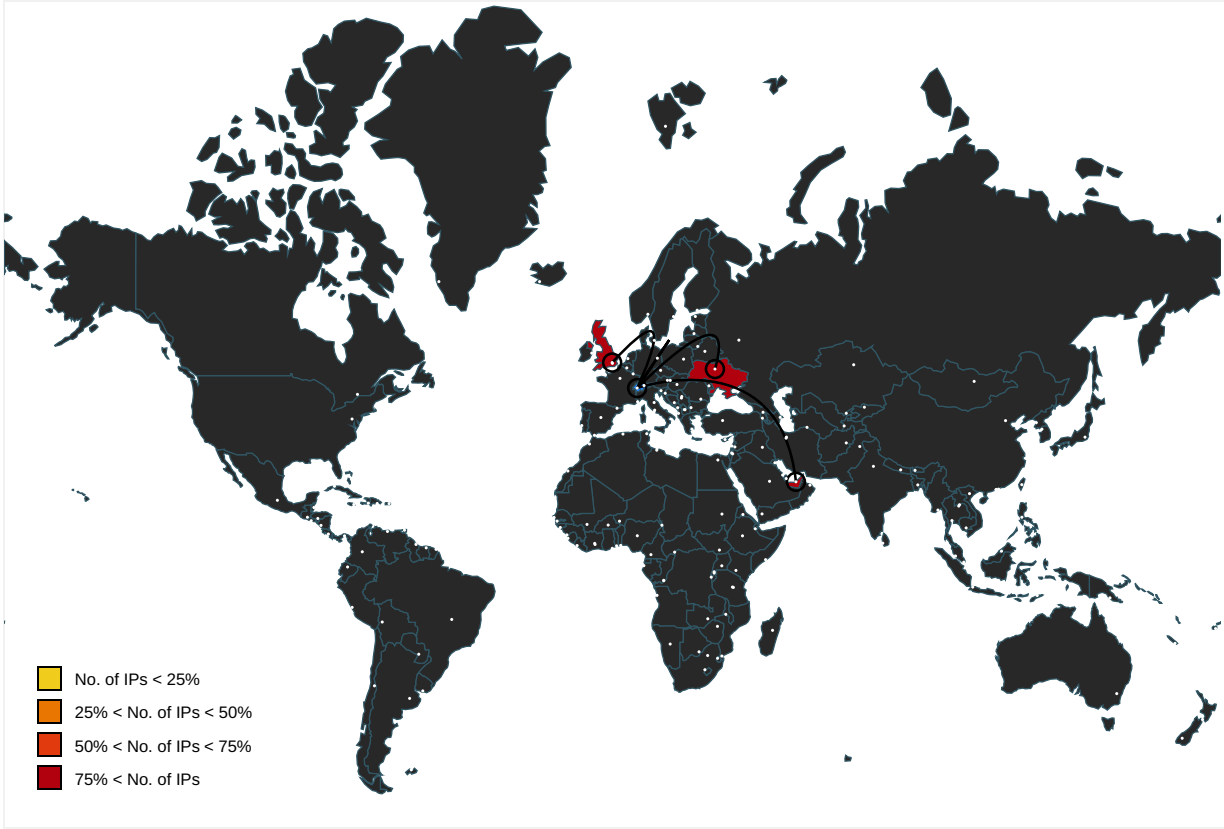
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.45.193.80/44313,6048108796.dat	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://45.144.31.232/44313,6048108796.dat	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.118.21.70	unknown	Ukraine		204957	GREENFLOID-ASUA	false
45.144.31.232	unknown	United Kingdom		42994	HQservCommunicationSolutionsIL	false
185.45.193.80	unknown	United Arab Emirates		60117	HSAE	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403443

Copyright Joe Security LLC 2021

Start date:	04.05.2021
Start time:	05:55:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9177284661-04302021.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)
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.expl.evad.winXLSM@1/7@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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	EgW5u2WYG2.exe	Get hash	malicious	Browse	• 45.134.255.99
	7IXb5bOTOQ.exe	Get hash	malicious	Browse	• 45.134.255.61
	DU61r0xvZ7.exe	Get hash	malicious	Browse	• 82.118.23.184
	TNT SHIPPING DOC 6753478364.exe	Get hash	malicious	Browse	• 91.90.195.7
	10ba8cb2_by_Libranalysis.exe	Get hash	malicious	Browse	• 195.123.238.191
	SThy2G7fGR.exe	Get hash	malicious	Browse	• 45.134.255.61
	65cb803d8339bc32863bd557a882cf2016ad7945b18f3.exe	Get hash	malicious	Browse	• 45.134.255.61
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.90.59.97
	kVXWdr5oFQ.exe	Get hash	malicious	Browse	• 195.123.233.63
	t.exe	Get hash	malicious	Browse	• 195.123.23 7.105
	scan-remittance-slip.xlsx	Get hash	malicious	Browse	• 82.118.23.217
	Shipping-Documents.xlsx	Get hash	malicious	Browse	• 82.118.23.217
	Remittance Advice - MA CONSULTING.xlsx	Get hash	malicious	Browse	• 82.118.23.217
	amCz0268Nl.exe	Get hash	malicious	Browse	• 45.134.255.61
	Contract_372758654-1.xlsm	Get hash	malicious	Browse	• 195.123.24 4.129
	Contract_372758654-1.xlsm	Get hash	malicious	Browse	• 195.123.24 4.129
	apr.21.A.31573147172-04202021.xlsm	Get hash	malicious	Browse	• 82.118.23.186
	O3UkuKlQ25.exe	Get hash	malicious	Browse	• 82.118.22.149
HSAE	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
	Static.dll	Get hash	malicious	Browse	• 185.183.96.157
	Static.dll	Get hash	malicious	Browse	• 185.183.96.157
	msals.dll	Get hash	malicious	Browse	• 185.183.96.157
	Payment_MT_103_#776363_Swift_Confirmation.exe	Get hash	malicious	Browse	• 185.244.15 0.183
	0303_15995446253021.doc	Get hash	malicious	Browse	• 185.183.96.157
	Static.dll	Get hash	malicious	Browse	• 185.183.96.157
	msals.dll	Get hash	malicious	Browse	• 185.183.96.157
	#U00d1#U00d1#U00d1#U00d0#U00bcBCCC.exe	Get hash	malicious	Browse	• 185.45.193.76
HQservCommunicationSolutionsIL	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	73827110_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 45.144.30.80
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	d658fc2e_by_Libranalysis.docm	Get hash	malicious	Browse	• 45.144.29.166
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	figure-04.26.2021.doc	Get hash	malicious	Browse	• 45.144.29.200
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	Anfrage-04.14.2021.doc	Get hash	malicious	Browse	• 91.194.11.70
	CompensationClaim-1416897608-04152021.xlsm	Get hash	malicious	Browse	• 45.144.30.16
	CompensationClaim-1416897608-04152021.xlsm	Get hash	malicious	Browse	• 45.144.30.16
	Suspect.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Compensation_690949256_04132021.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Suspect.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	Compensation_690949256_04132021.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	malw.xlsm	Get hash	malicious	Browse	• 45.144.30.106
	malw.xlsm	Get hash	malicious	Browse	• 45.144.30.106

JA3 Fingerprints

No context

Dropped Files

No context

Copyright Joe Security LLC 2021

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EB62A569.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=5], baseline, precision 8, 1080x1080, frames 3
Category:	dropped
Size (bytes):	92379
Entropy (8bit):	7.654577060340879
Encrypted:	false
SSDEEP:	1536:1o1vutINbjOXGw548LBkVb/oyrKXkX89DcO9GQSnIv+C1EDFVxkR7Y90:wvKINbjvw548LMb/oqKO8NnS8+60Kc0
MD5:	4A425E6A5A885C0D0E2589506FD2244B
SHA1:	E23482422480A4720E22F311B42BD65E2F3556F8
SHA-256:	76E685FC2035D8CF19945C6686D82054B64D0A9612853D8F428C4B4FE351C160
SHA-512:	3C827E13A12CC817CBD80EA7C89BEC5288FD21250728E76E00D6355008F704C77EC9BC37C85FF076D8D1F960DB53741F352AB649CD2C754B71B4D11CFFBEEA4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`.....ZExif..MM.*.....J.....Q.....Q.....Q.....C.....C.....8.8..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..D.G.\.....i].....k.@U.....B..Hw.A...`p;.RsIRHTs..%G?QU.#..$..."...U.A....g].s.....c.,....{W'..M.Nc....F.~..y..l..`.e..a..[...P.y]..k_..Cl..z.Ru..s.6.Y....."..1]Q.....e#.....~.`sk..KH.....p.4.i.j+3{.....N.DS..L.....o..o.5f>..jY.uS...Z.B...UG`)..6D....(.....

C:\Users\user\AppData\Local\Temp\46FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	118458
Entropy (8bit):	7.69393685758773
Encrypted:	false
SSDEEP:	3072:Gmk7zcrvKINbjvw548LMb/oqKO8NnS8+60Kcu:GXsmAbT648LM7D98Np+Ej
MD5:	B261F57D31845D480C8A1AFAD889CD8B
SHA1:	D7265E552FE0419D658F8B54F576B23FC314003B
SHA-256:	B9146B6A8983A61E7E0DC388A31129156A2674D2CB9C76C01A1F609B229E3B68
SHA-512:	C8674C1D37DAC1463BC3C3B46D7A91E7AB96805FA8FFCC42B8EDE3217084CB859D73D49BEF917F478A7FF624BF8B6F14D259164A741EF66B46C496F87A75EB38
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?..."....r.y...I>.&..m.$H...K...$$@.zQ;.3\p..V.K.AYS..:"..a.2uE...._.....5P.5.r=..m..v...6."M..7cA4..@...+3.[.....q..5.....k".X.A&.[.....~.t2U..7...UE.sZ...Q.4..... .xi.....VS..2.G.....rz.a..V....Xh..?P....rZ.....T..;..._.A.$....?.E..J.W..Sk..<or..%..h.-.-....>.k\.7Qg.re`.v.....$.....5d.....4?{.:.&...._?>?.....B.-CFu....p..1.T.z..cw.!=.M-....}.....3..7...r.....;ap.7.B.e.N[...v.....z..T]:.....c.`.Nx....W.<..r.O.....PK.....!.....*.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\9177284661-04302021.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 14:08:21 2020, mtime=Tue May 4 11:56:48 2021, atime=Tue May 4 11:56:48 2021, length=118468, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.513586876217989
Encrypted:	false
SSDEEP:	24:8L948/XT46kZOBep6Dv3qodM7dD2L948/XT46kZOBep6Dv3qodM7dV:868/XTDkZEmoQh268/XTDkZEmoQ/
MD5:	06FA078A531765C1007CEE0C3511105A
SHA1:	D9CAB1BF432B30B21685B10BF29BACE893219EB7
SHA-256:	D4D768500197C2D5CC85168B570CBBF6E03858D0B71861CE63E47697331FBACE
SHA-512:	25EA0E863D10485A0FB49E8CEAA40A10DEF0F61D20C5C32C7654123B6BE889434B04B4959153307477A5E1B062673996B597E500F502491DDA0D5FDB548C226A
Malicious:	false
Reputation:	low
Preview:	L.....F.... ..._..{..!t...@..B....@.....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.....z.2.....R.g .917728~1.XLS..^.....Q.y.Q.y*...8.....9.1.7.7.2.8.4.6.6.1.-.0.4.3.0.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\9177284661-04302021.xlsm./.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.9.1.7.7.2.8.4.6.6.1.-.0.4.3.0.2.0.2.1...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.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....134349.....D_..

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=Tue May 4 11:56:48 2021, atime=Tue May 4 11:56:48 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.484024614599478
Encrypted:	false
SSDEEP:	12:85Q+H0LgXg/XAlCPCHaXIB8kB/KWUbX+WnicvbxbDtZ3YilMMEpxRljK2yTdJP9O:855Hi/XT46kkBYexDv3qorNru/
MD5:	282B9BA9B10CBE105F6C4232BA7F1CA3
SHA1:	49CC608F1C3B14C767AA1FC1556C8BD862D59827
SHA-256:	02F266B0E8F26FF1BCE8757C82BC15740E8D13B6A91CD6C3D753DE3B5E5197AD
SHA-512:	C948145A4C9906512C44482F8E1B31478BE6DC09AE420B1F4012F44DFAAF34DFCC15FA8F240C954A078D2E0B33A5258397104EADD4ABD6BC9E7A8568E256E1D B
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..!t...@..!t...@...0.....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.....R.g..Desktop.d.....QK.X.R.g*..._=.....:.....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\..#.....\\134349\Users.user\Desktop.....\.....\.....\.....\.....\D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.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.....134349.....D_....3N...W...9r.[.*.....}EkD_....3N.. .W...9r.[.*.....}Ek....

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):	112
Entropy (8bit):	4.517286360501819
Encrypted:	false
SSDEEP:	3:oyBVomxW7SNRfRg9rlNRfRg9rlmxW7SNRfRg9rlv:djQc2pZ2pZc2p1
MD5:	3C738600E2C168DA464E5F6B8D1F5BFE
SHA1:	B8A71D217EFB558FAAA522D9F116879690781851
SHA-256:	B426222C318FCE644598521ECE3647859958E71F0B282931B26E02193B2BC4E0
SHA-512:	4E9DA68D7BA28E7FD8B14F57CD85CE1BECDD1DE65C95E35976DCB98C57F6105ED51553D016BEAC78892A57F318E4A47D314A368C13AFC45F176E18836BAB4 C0
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..9177284661-04302021.LNK=0..9177284661-04302021.LNK=0..[misc]..9177284661-04302021.LNK=0..

C:\Users\user\Desktop\27FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	118468
Entropy (8bit):	7.693044301214109
Encrypted:	false
SSDEEP:	3072:GmkkSrvKINbjvw548LMb/oqKO8NnS8+60KcL:GXvmAbT648LM7D98Np+Ea
MD5:	D755F6BF4545DC55ED533503A6B57A15
SHA1:	2A83D57F391F14D257BF24D4B56652A303E732D2
SHA-256:	28E205CEA6A4CF3B166245FD8248689F81E52E80D7F3984157107A51CC9C59A3
SHA-512:	0CF590A357DDB1872AE53394A6794B927A64545DDEA9F20FC056A1B19EDFAC0B774A394E5BD5996B208E3A081F23897877B3F7ADB2D54E93C159B686E5AF4F9
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\Desktop\~$9177284661-04302021.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false

C:\Users\user\Desktop\~$9177284661-04302021.xlsm	
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):	7.679226664040162
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:	9177284661-04302021.xlsm
File size:	114788
MD5:	a8b4e37766d35b543884d8882147eaa2
SHA1:	4356c14118ea9098dabb6d9af620003b7929058a
SHA256:	533c8713c4e10c223a9f8139f9d408ca326aee14a1d88382c91f2ff18cf0f93c
SHA512:	581ee69b843a7657677e1f6b74147f273f340474ff36de56b1d579d0364ccc6c27c2f9dedf4d855bc2841351957a3620dc0327153ff4ff3dc87a2c6ad7eb8a6f
SSDEEP:	3072:K6vKINbjvw548LMb/oqKO8NnS8+60Kcxtc:6AbT648LM7D98Np+Et
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/403443/sample/9177284661-04302021.xlsm"

Indicators

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

Summary

Author:	Rabota
Last Saved By:	Noped
Create Time:	2015-06-05T18:19:34Z
Last Saved Time:	2021-04-30T08:26:34Z
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: Byutut.bas, Stream Size: 1343

General	
Stream Path:	VBA/Byutut
VBA File Name:	Byutut.bas
Stream Size:	1343
Data ASCII:	. . . . . ; G . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 03 f0 00 00 00 e2 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 10 03 00 00 b0 04 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 08 00 ff ff 00 00 00 00 00 00 00

Keyword
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: PROJECT, File Type: ISO-8859 text, with CRLF line terminators, Stream Size: 543

General	
Stream Path:	PROJECT
File Type:	ISO-8859 text, with CRLF line terminators
Stream Size:	543
Entropy:	5.37319650849
Base64 Encoded:	True
Data ASCII:	I D = " { 6 5 E C 9 F D C - 2 0 9 0 - 4 6 C 0 - 8 5 8 F - 4 1 2 6 6 D 3 E 0 1 6 B } " . . D o c u m e n t = ... / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = ... 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = B y u t u t . . D o c u m e n t = ... 2 / & H 0 0 0 0 0 0 0 0 . . C l a s s = C l a s s 1 . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " 0 9 0 B D 9 D F D D D F D D D F D D D F D D
Data Raw:	49 44 3d 22 7b 36 35 45 43 39 46 44 43 2d 32 30 39 30 2d 34 36 43 30 2d 38 35 38 46 2d 34 31 32 36 36 44 33 45 30 31 36 42 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d dd f2 e0 ca ed e8 e3 e0 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d cb e8 f1 f2 31 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 cb e8

Stream Path: PROJECTwm, File Type: data, Stream Size: 107

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	107
Entropy:	3.96151942936
Base64 Encoded:	False
Data ASCII:	. . . . . - . B . 0 . . . = . 8 . 3 . 0 . . . . . 1 . . . 8 . A . B . 1 . . . B y u t u t . B . y . u . t . u . t . . . . . 2 . . . 8 . A . B . 2 . . . C l a s s 1 . C . l . a . s . s . 1 . . . . .
Data Raw:	dd f2 e0 ca ed e8 e3 e0 00 2d 04 42 04 30 04 1a 04 3d 04 38 04 33 04 30 04 00 00 cb e8 f1 f2 31 00 1b 04 38 04 41 04 42 04 31 00 00 00 42 79 75 74 75 74 00 42 00 79 00 75 00 74 00 75 00 74 00 00 00 cb e8 f1 f2 32 00 1b 04 38 04 41 04 42 04 32 00 00 00 43 6c 61 73 73 31 00 43 00 6c 00 61 00 73 00 73 00 31 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2831

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2831
Entropy:	4.1308794712
Base64 Encoded:	False
Data ASCII:	. a . . . . .

General	
Entropy:	3.30953727146
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ ` . . . . . " . . . . . Q . . . . . b T Z . . F . v . V . e . . . . .
Data Raw:	93 4b 2a b2 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 146

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	146
Entropy:	1.48909835582
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . j . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 11 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 170

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	170
Entropy:	1.65437585425
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . @ . . . . . ~ x . . . . . a . . . . . Z . . . 2 . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff 0c 00 00 00 00 00 00 12 00 00

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 156

General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	156
Entropy:	1.63365900945
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . ` . . . . . b . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: VBA/dir, File Type: data, Stream Size: 601

General	
Stream Path:	VBA/dir
File Type:	data
Stream Size:	601
Entropy:	6.45605461621
Base64 Encoded:	True
Data ASCII:	. U . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . O ~ 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 . -

General	
Data Raw:	01 55 b2 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 a6 4f 7e 62 05 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

Stream Path: VBA/\x1051\x1080\x1089\x10901, File Type: data, Stream Size: 990

General	
Stream Path:	VBA/\x1051\x1080\x1089\x10901
File Type:	data
Stream Size:	990
Entropy:	3.19675892958
Base64 Encoded:	True
Data ASCII:	. . . . . - . . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 1c cc 1e a1 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-05:56:49.914165	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	185.45.193.80	192.168.2.22
05/04/21-05:57:32.232736	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	45.144.31.232	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 05:56:49.601764917 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:56:49.659508944 CEST	80	49165	185.45.193.80	192.168.2.22
May 4, 2021 05:56:49.659672976 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:56:49.660406113 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:56:49.718135118 CEST	80	49165	185.45.193.80	192.168.2.22
May 4, 2021 05:56:49.914165020 CEST	80	49165	185.45.193.80	192.168.2.22
May 4, 2021 05:56:49.914295912 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:56:49.966447115 CEST	49166	80	192.168.2.22	82.118.21.70
May 4, 2021 05:56:52.975069046 CEST	49166	80	192.168.2.22	82.118.21.70
May 4, 2021 05:56:58.981699944 CEST	49166	80	192.168.2.22	82.118.21.70
May 4, 2021 05:57:10.996073961 CEST	49167	80	192.168.2.22	82.118.21.70
May 4, 2021 05:57:14.005753040 CEST	49167	80	192.168.2.22	82.118.21.70
May 4, 2021 05:57:20.012283087 CEST	49167	80	192.168.2.22	82.118.21.70
May 4, 2021 05:57:32.057816029 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:57:32.139307976 CEST	80	49168	45.144.31.232	192.168.2.22
May 4, 2021 05:57:32.139580011 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:57:32.140759945 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:57:32.222258091 CEST	80	49168	45.144.31.232	192.168.2.22
May 4, 2021 05:57:32.232736111 CEST	80	49168	45.144.31.232	192.168.2.22
May 4, 2021 05:57:32.232819080 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:57:54.979974985 CEST	80	49165	185.45.193.80	192.168.2.22
May 4, 2021 05:57:54.980161905 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:58:37.235938072 CEST	80	49168	45.144.31.232	192.168.2.22
May 4, 2021 05:58:37.236006021 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:58:49.502119064 CEST	49168	80	192.168.2.22	45.144.31.232
May 4, 2021 05:58:49.502490997 CEST	49165	80	192.168.2.22	185.45.193.80
May 4, 2021 05:58:49.560103893 CEST	80	49165	185.45.193.80	192.168.2.22
May 4, 2021 05:58:49.583354950 CEST	80	49168	45.144.31.232	192.168.2.22

HTTP Request Dependency Graph

- 185.45.193.80
- 45.144.31.232

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.45.193.80	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:56:49.660406113 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: 185.45.193.80 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:56:49.914165020 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 03:56:49 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	49168	45.144.31.232	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 05:57:32.140759945 CEST	2	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: 45.144.31.232 Connection: Keep-Alive
May 4, 2021 05:57:32.232736111 CEST	3	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Tue, 04 May 2021 03:57:32 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2388 Parent PID: 584

General

Start time:	05:56:45
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:	0x13f7c0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F40F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13FB0EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\46FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAE09AC0	unknown
C:\Users\user\Desktop\~$9177284661-04302021.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	7FEEAE09AC0	unknown
C:\Users\user\Desktop\27FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAE09AC0	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	URLDownloadToFileA

Copyright Joe Security LLC 2021

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	1404E828C	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	1404E828C	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	1404E828C	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	1404E828C	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F40F.tmp	success or wait	1	13FD7B818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\46FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAE09AC0	unknown
C:\Users\user\Desktop\27FE0000	C:\Users\user\Desktop\9177284661-04302021.xlsml	success or wait	1	7FEEAE09AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$9177284661-04302021.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 20 20	.user	success or wait	1	13FA0F526	WriteFile
C:\Users\user\Desktop\~$9177284661-04302021.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\46FE0000	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	7FEEAE09AC0	unknown
C:\Users\user\AppData\Local\Temp\46FE0000	1048	2	03 00	..	success or wait	25	7FEEAE09AC0	unknown
C:\Users\user\AppData\Local\Temp\46FE0000	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\46FE0000	7662	4096	ec 7c 0b 7c 54 55 7e ff b9 77 6e 92 49 48 c2 24 06 36 02 c2 65 12 20 40 12 26 93 30 79 48 64 1e 99 90 68 42 30 41 a4 6e 34 99 49 06 08 4e 66 c2 cc 04 83 0f 98 24 ac 8b ae 5d 11 b7 ea ba 6e 0b ea 76 5d 5f 8b ae dd ca 76 d7 4d 7c af a5 55 b7 6e 17 b7 db 0a 3e ba d6 d6 0a 6d fd d4 5a d7 fc bf bf 7b ee 99 b9 19 02 04 ec 63 ed df 93 7c ef f9 dd df f9 9d df 79 bf ef 99 57 5e ce 3b 7a e0 b1 39 c7 58 8a b9 88 99 d8 a7 13 99 2c dd c0 97 40 13 34 63 61 4c 06 41 f8 74 62 62 42 e3 e1 01 f2 0b f3 39 ca 81 df 22 ae 19 28 b7 85 80 02 a4 01 54 e6 66 20 1b c8 04 b2 80 19 c0 4c 60 1e 90 0b 50 99 5b 60 e7 01 f9 c0 05 40 01 30 0b 98 0d 7c 09 28 04 ce 07 e6 00 73 81 1c a0 04 98 0f 2c 00 54 c0 0a 90 ae 22 d8 c5 c0 22 60 31 b0 04 58 0a d8 80 65 c0 72 a0 14 28 03 ca 81 15 40 05	.|.|TU~..wn.IH.$.6..e. @.&.0yH d...hB0A.n4.I..Nf.....$...]. ..n..v]_....v.M|..U.n....>.... m..Z....{.....c...|.....y. ..W^.;z..9.X.....,...@.4caL .A.tbbB.....9..."..(.....T.f .....L`...P.[`.....@.0...|. (.....s.....,.T...."..."`1..X ...e.r..(....@.	success or wait	3	7FEEAE09AC0	unknown
C:\Users\user\AppData\Local\Temp\46FE0000	17769	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\46FE0000	116587	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 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 4f ee 6b a3 78 02 00 00 75 04 00 00 0f 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..-.....!. O.k.x...u..... xl/workbook.xml	success or wait	1	7FEEAE09AC0	unknown
C:\Users\user\Desktop\~$9177284661-04302021.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 20 20	.user	success or wait	1	13FA0F526	WriteFile
C:\Users\user\Desktop\~$9177284661-04302021.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\27FE0000	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	7FEEAE09AC0	unknown
C:\Users\user\Desktop\27FE0000	1048	2	03 00	..	success or wait	25	7FEEAE09AC0	unknown
C:\Users\user\Desktop\27FE0000	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\27FE0000	7662	4096	ec 7c 0b 7c 54 55 7e ff b9 77 26 c9 24 24 30 89 81 8d 80 70 99 04 08 90 84 99 49 18 92 48 64 9e 21 d1 84 60 82 48 dd 68 32 93 0c 10 9c cc 84 99 09 06 1f 30 49 58 17 5d bb a2 6e d5 75 6d 0b ea 76 5d 5f 8b ae dd ca 76 d7 4d 7c af a5 15 b7 6e 17 b7 db 0a 3e ba d6 d6 0a 6d fd d4 5a d7 fc bf bf 7b ee 99 b9 33 04 08 b8 6d d7 fe 3d c9 f7 9e df fd 9d df f9 9d f7 fb 9e 39 fc 4a e1 d1 fd 8f cf 3e c6 32 cc 45 cc c0 3e 9d c8 65 d9 3a be 04 9a a0 1a 33 63 32 08 c2 a7 13 13 13 2a 0f 0f 90 5f 98 cf 51 0e fc 06 71 cd 41 b9 2d 00 8c 40 16 40 65 6e 02 f2 81 5c 20 0f 98 06 cc 00 e6 02 d3 01 2a 73 33 ec 42 a0 08 b8 00 28 06 66 02 b3 80 2f 01 25 c0 f9 c0 6c 60 0e 50 00 94 03 f3 80 f9 80 02 58 00 d2 55 0a bb 0c 58 08 2c 02 16 03 4b 00 2b b0 14 58 06 54 00 95 40 15 b0 1c b0 01	.|.|TU~..w&.$$0....p.....I..Hd.!..`.H.h2.....0IX.]..n.um..v]_....v.M|....n....>....m..Z....{...3...m..=..... .9.J.....>.2.E..>..e.:.....3c2 .....*..._..Q...q.A.-..@.@en. ..\ .....*s3.B....(.f.../. %...l`.P.....X..U...X.,...K .+..X.T..@.....	success or wait	3	7FEEAE09AC0	unknown
C:\Users\user\Desktop\27FE0000	17779	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\Desktop\27FE0000	116597	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 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 4f ee 6b a3 78 02 00 00 75 04 00 00 0f 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..-.....!. O.k.x...u..... xl/workbook.xml	success or wait	1	7FEEAE09AC0	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EB62A569.jpg	0	65536	success or wait	1	7FEEAE09AC0	unknown
C:\Users\user\Desktop\9177284661-04302021.xlsm	unknown	8	success or wait	1	7FEEAE09AC0	unknown
C:\Users\user\Desktop\9177284661-04302021.xlsm	0	8	pending	1	7FEEAE09AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAE1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAE1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAE1E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	5	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	5	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF44E	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF557	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF602	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF6DD	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF779	success or wait	1	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAE09AC0	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	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	3	7FEEAE09AC0	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\3764832265.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8138487229.xlsx	success or wait	3	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8300215382.xlsx	success or wait	3	7FEEAE09AC0	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\EF44E	EF44E	binary	04 00 00 00 54 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 33 00 2E 00 36 00 37 00 2E 00 33 00 32 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 B3 D0 68 F1 E4 40 D7 01 4E F4 0E 00 4E F4 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\EF557	EF557	binary	04 00 00 00 54 09 00 00 39 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 34 00 2E 00 31 00 30 00 2E 00 36 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 B3 D0 68 F1 E4 40 D7 01 57 F5 0E 00 57 F5 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\EF602	EF602	binary	04 00 00 00 54 09 00 00 38 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 35 00 2E 00 36 00 2E 00 37 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 78 A9 93 F1 E4 40 D7 01 02 F6 0E 00 02 F6 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\4144085054.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2849925037.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0353475199.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8138487229.xlsx	success or wait	2	7FEEAE09AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8300215382.xlsx	success or wait	2	7FEEAE09AC0	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\EF6DD	EF6DD	binary	04 00 00 00 54 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 1F 69 CA F1 E4 40 D7 01 DD F6 0E 00 DD F6 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\EF779	EF779	binary	04 00 00 00 54 09 00 00 2F 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 39 00 31 00 37 00 37 00 32 00 38 00 34 00 36 00 36 00 31 00 2D 00 30 00 34 00 33 00 30 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 42 98 E4 F1 E4 40 D7 01 79 F7 0E 00 79 F7 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00

Disassembly