ID: 636
Sample Name:
2021_0002565_DDT.xls
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 17:48:23
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

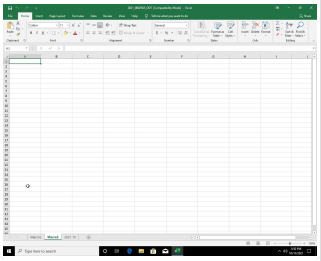
Windows Analysis Report 2021_0002565_DDT.xls

Overview

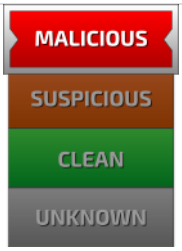
General Information

Sample Name:	2021_0002565_DDT.xls
Analysis ID:	636
MD5:	5b239ac2b45218..
SHA1:	abefd9905f25fdc…
SHA256:	f3ff9603b23796a…

Most interesting Screenshot:



Detection



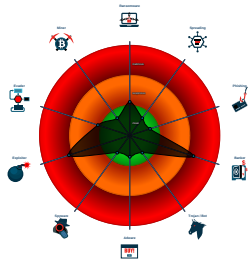
Ursnif Dropper

Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Italy targeted Ursnif droppe…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Process Tree

- **System is start**
- EXCEL.EXE (PID: 2620 cmdline: 'C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE' 'C:\Users\alfredo\Desktop\2021_0002565_DDT.xls' MD5: 23CAD504B3E04BB54CD636AD2874041A)
- **cleanup**

Yara Overview

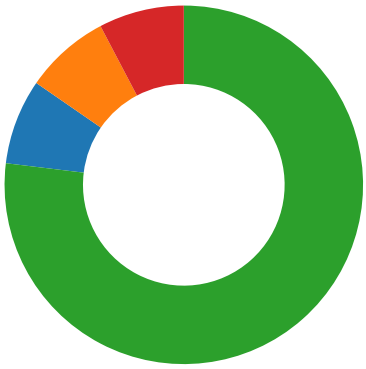
No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

- Software Vulnerabilities
- E-Banking Fraud
- System Summary
- Hooking and other Techniques for Hiding and Protection



Click to jump to signature section

E-Banking Fraud:

Detected Italy targeted Ursnif dropper document

System Summary:

Document contains an embedded VBA macro with suspicious strings

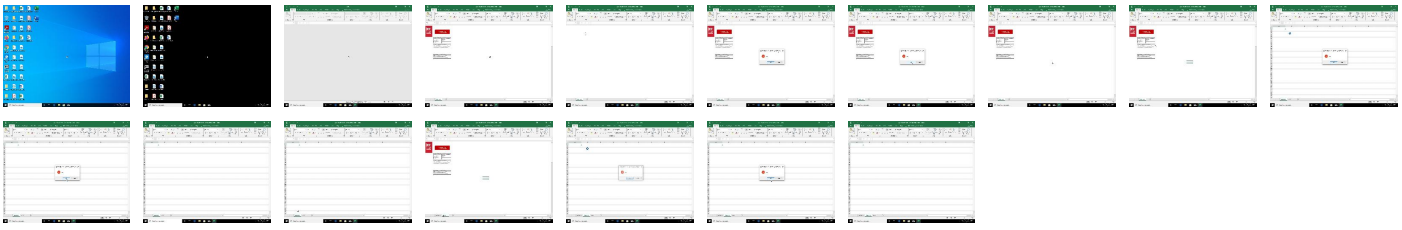
Mitre Att&ck Matrix

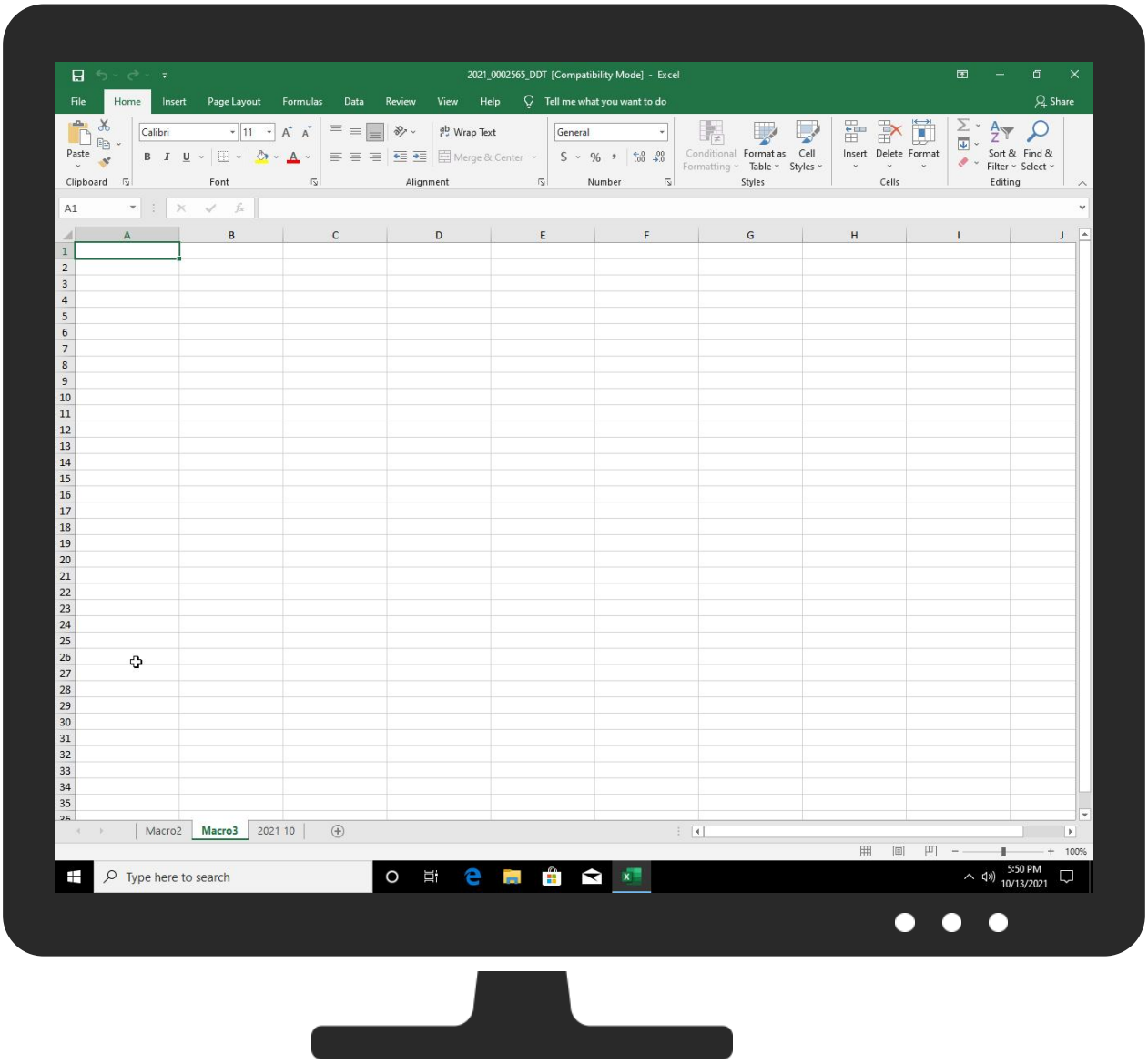
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Scripting 1 1	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 1 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

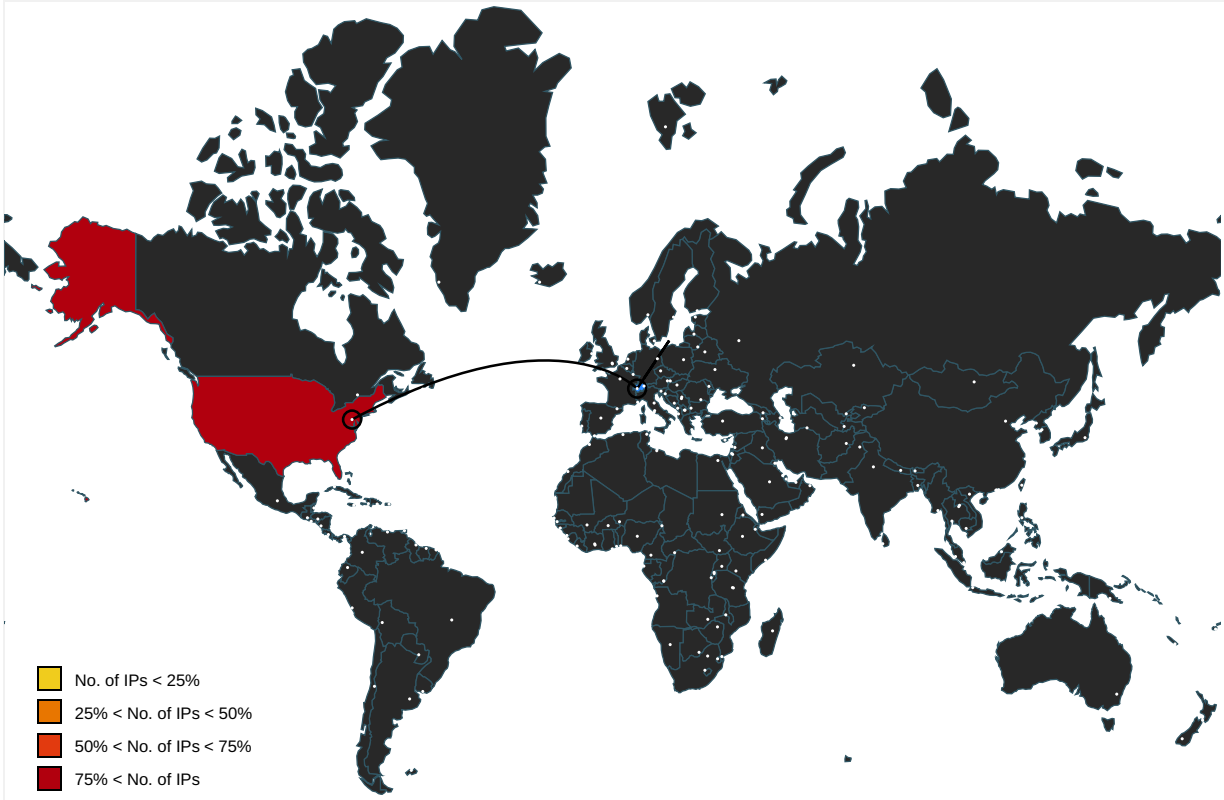
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.113.194.132	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.88.177	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.28.63	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.21.140.114	unknown	European Union		16625	AKAMAI-ASUS	false
20.50.201.195	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.88.34	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	636
Start date:	13.10.2021
Start time:	17:48:23
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	2021_0002565_DDT.xls
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Detection:	MAL
Classification:	mal52.bank.expl.winXLS@1/8@0/72
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls
Warnings:	Show All • Exclude process from analysis (whitelisted): svchost.exe • Excluded IPs from analysis (whitelisted): 40.126.31.6, 40.126.31.143, 40.126.31.4, 20.190.159.136, 40.126.31.1, 40.126.31.8, 20.190.159.134, 40.126.31.135, 20.190.160.67, 20.190.160.69, 20.190.160.73, 20.190.160.8, 20.190.160.71, 20.190.160.75, 20.190.160.2, 20.190.160.4, 40.126.31.139, 40.126.31.141, 20.190.159.138, 20.190.159.132 • Excluded domains from analysis (whitelisted): login.live.com, www.tm.lg.prod.aadmsa.akadns.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	379722
Entropy (8bit):	4.9088149211082355
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	{"MajorVersion":4,"MinorVersion":17,"Expiration":14,"Fonts":[{"a":[4294966911],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32696,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23643452060","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22180,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17656736728","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294966911],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54372,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"31150835240","p":[2,11,8,4,2,2,2,2,2,4],"sub":[],"t":"ttf","u":[3,0,0,0],"v":67502,"w":45875968},{"c":[536870913,0],"dn":"Agency FB","fs":52680,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"29260917085","p":[2,11,5,3,2,2,2,2,

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview_4_17.ttf	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	TrueType Font data, 10 tables, 1st "OS/2", 7 names, Microsoft, language 0x409, \251 2018 Microsoft Corporation. All Rights Reserved.msofp_4_17RegularVersion 4.17;O365
Category:	dropped
Size (bytes):	672416
Entropy (8bit):	6.566110770587873
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview_4_17.ttf	
Preview:	..... OS/29.P...(...`cmap.s.....pglyf..e.....0.head-@;,.....6hheaE.@B.....$hmtx.....ploca..@....h...tmaxp..... name.T+...A\|....post...<..B.... .....Me.._.<.....<.. .....Aa.x.....Q....Aa....Aa.....~.....j.....3.....MS .@.....(...Q..... .....d.....0...J.....8...>.....+a..# ...,.....K.....z.....N.....*..!..-...+....z.....h..%^..3...&j..+...+%..".....l.....$A...,.....g...&...=.....X..&.....*.....&...(B.....#.....j.....+...P...5. ..@...).....#.....*...N...7.....<...;>.....].....5.....#....s.....$.....$.....^.....H.....%...7.....6.....O...V.....K.....c.....!.....$...&...*p..+<..+...-.... q.....O.....F..(....5..0K..$...0V...k..*e...o.....S...*...0..0...*M.....9...

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D01F1074-7A8E-4E0B-A1C2-7BFA61CB3A1A	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	139380
Entropy (8bit):	5.357962258943721
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-10-13T15:49:30">.. Build: 16.0.14604.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\excel.exe_Rules.xml	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	313927
Entropy (8bit):	5.173295416823414
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d 448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159" G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L><R> <O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N=" ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.8556249257072412
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres	
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".C.J.1.m.u.g.S.o.z.s.S.9.x.S.Z./.Q.v.O.c.+.E.J.4.u.2.c.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.M.v.C.v.J.3.A.1.w.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.l.+.s.B.A.A.A.A.r.B.z.X.D.z.

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\9aad439831564ef9f88438a70a63c87e26ef3852.tbres	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	3902
Entropy (8bit):	3.990812285105349
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".m.q.1.D.m.D.F.W.T.v.n.4.h.D.i.n.C.m.P.I.f.i.b.v.O.F.I.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".q.t.0.9.o.p.X.A.1.w.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.w.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.l.+.s.B.A.A.A.A.r.B.z.X.D.z.

C:\Users\alfredo\AppData\Roaming\Microsoft\Office\Recent\2021_0002565_DDT.LNK	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Jun 8 14:37:17 2021, mtime=Wed Oct 13 23:49:32 2021, atime=Wed Oct 13 23:49:26 2021, length=51712, window=hide
Category:	dropped
Size (bytes):	547
Entropy (8bit):	4.669580883850226
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	L.....F.... ......)\....Y.....`V.....x.v.2.....NS.. .2021_0~1.XLS..Z.....R.|NS.....U.....V:..2.0.2.1._.0.0.0.2.5.6.5._.D.D.T...x.l.s.....\.....-.....[.....;S.....C:\Users\alfredo\Desktop\2021_0002565_DDT.xls..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.2.0.2.1._.0.0.0.2.5.6.5._.D.D.T...x.l.s.`.....X.....715575.....N...n..O...}R... ..Km.....).].N...n..O...}R... ..Km.....).].E.....9...1SPS..mD..pH.H@..=x.....h....H....F.5./EG.gM.U.....

C:\Users\alfredo\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.548813030410997
Encrypted:	false
SSDEEP:	
MD5:	D41D8CD98F00B204E9800998ECF8427E
SHA1:	DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
SHA-256:	E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855
SHA-512:	CF83E1357EEFB8BDF1542850D66D8007D620E4050B5715DC83F4A921D36CE9CE47D0D13C5D85F2B0FF8318D2877EEC2F63B931BD47417A81A538327AF927DA3
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..2021_0002565_DDT.LNK=0..[xls]..2021_0002565_DDT.LNK=0..

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Create Time/Date: Mon Oct 11 09:03:47 2021, Last Saved Time/Date: Mon Oct 11 09:03:49 2021, Security: 0, Comments: "BRT
Entropy (8bit):	5.314831852450583
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	2021_0002565_DDT.xls
File size:	51712
MD5:	5b239ac2b45218ad505553d52203c744
SHA1:	abefd9905f25fdcea76783cfd877c19206d117ab
SHA256:	f3ff9603b23796a30d10ae2cfa0001212752705a3e602371ae74d0f4d8defb71
SHA512:	af1bb5477e46cc4ed1177a0b48a6d187b2a45fa68a28291f10466d85816bae8d6ba1ad1579f1b1f6ef4d276ad73efd98cebf4fe7071349769c6a93dc0cbda5fd
SSDEEP:	1536:dsQlYkEIbSkKBEqEXPgsRZmbaoFhZhR0cixIHm0THPFDI0LF/yUKAmsiwc:dhlYkEIuPm3fNRZmbaoFhZhR0cixIHmP
File Content Preview:	.....>.....;..... ....

File Icon

Icon Hash:	74f4e4c2cec4c0d4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "2021_0002565_DDT.xls"

Indicators

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

Summary

Code Page:	1252
Comments:	"BRT
Create Time:	2021-10-11 08:03:47.102000
Last Saved Time:	2021-10-11 08:03:49
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False

Document Summary

Application Version:	1048576

Streams with VBA

VBA File Name: Foglio1, Stream Size: 992

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Foglio1
VBA File Name:	Foglio1
Stream Size:	992
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 b8 98 9f 83 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

VBA File Name: Questa_cartella_di_lavoro, Stream Size: 6050

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Questa_cartella_di_lavoro
VBA File Name:	Questa_cartella_di_lavoro
Stream Size:	6050
Data ASCII:	. . . . . 2 . . . . . ` . . . n . . . b . . . . . l . . . . . # . . . . . p . . . . . F . . . w . K . f . . . . . : . . . . . F . . . . . ` . . J . . . . ~ . . . . . x . . . . . ` . . J . . . . . ~ . . . F . . . w . K . f . . . . : . . . . . M E . . . . .
Data Raw:	01 16 03 00 06 00 01 00 00 32 0b 00 00 e4 00 00 00 10 02 00 00 60 0b 00 00 6e 0b 00 00 62 13 00 00 0e 00 00 00 01 00 00 00 b8 98 6c 8d 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 70 00 ff ff 00 00 1c 46 db f0 90 77 d1 4b a7 66 e3 9c a9 9f 00 3a 19 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 00 46 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 118

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	118
Entropy:	4.32915524493
Base64 Encoded:	True
Data ASCII:	. . . . . F * . . . (F o g l i o d i l a v o r o d i M i c r o s o f t E x c e l 2 0 0 3 . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 2a 00 00 00 28 46 6f 67 6c 69 6f 20 64 69 20 6c 61 76 6f 72 6f 20 64 69 20 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 248

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	248
Entropy:	2.78187154374
Base64 Encoded:	True
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . 2 0 2 1 1 0 . . . . . F o g l i d i l a v o r o . . . . .

General	
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c8 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 a0 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 160

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	160
Entropy:	3.0437641747
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . p . . . . 8 . . . . @ . . . . . . L . . . . X . . . . ` . . . . @ . . . . v . . . @ . . . . v . . . . ' ' B R T . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 70 00 00 00 05 00 00 00 01 00 00 00 38 00 00 00 0c 00 00 00 40 00 00 00 0d 00 00 00 4c 00 00 00 13 00 00 00 58 00 00 00 06 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 e4 04 00 00 40 00 00 00 e0 03 9d 84 76 be d7 01 40 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 28527

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	28527
Entropy:	6.28607255882
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . B . . . . . a . . . . = ... Q u e s t a _ c a r t e l l a _ d i _ l a v o r o . . . . = ... C
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 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 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

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 454

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	454
Entropy:	5.34024688628
Base64 Encoded:	True
Data ASCII:	I D = " { 4 5 6 C 0 9 9 E - 4 D E E - 4 4 5 9 - 9 9 9 E - 2 4 3 6 C D 6 1 0 0 B 1 } " . . D o c u m e n t = Q u e s t a _ c a r t e l l a _ d i _ l a v o r o / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F o g l i o 1 / & H 0 0 0 0 0 0 0 0 . . 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 = " 8 0 8 2 5 2 5 0 5 6 5 0 5 6 5 0 5 6 5 0 5 6 " . . D P B = " 2 6 2 4 F 4 5 0 3 C 5 0 E 3 5 1 E 3 5 1 E 3 " . . G C = "
Data Raw:	49 44 3d 22 7b 34 35 36 43 30 39 39 45 2d 34 44 45 45 2d 34 34 35 39 2d 39 39 39 45 2d 32 34 33 36 43 44 36 31 30 30 42 31 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 6f 67 6c 69 6f 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 56

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 104

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	104
Entropy:	3.33133492199
Base64 Encoded:	False
Data ASCII:	Q u e s t a _ c a r t e l l a _ d i _ l a v o r o . Q . u . e . s . t . a . _ . c . a . r . t . e . l . l . a . _ . d . i . _ . l . a . v . o . r . o . . . F o g l i o 1 . F . o . g . l . i . o . 1 . . . . .
Data Raw:	51 75 65 73 74 61 5f 63 61 72 74 65 6c 6c 61 5f 64 69 5f 6c 61 76 6f 72 6f 00 51 00 75 00 65 00 73 00 74 00 61 00 5f 00 63 00 61 00 72 00 74 00 65 00 6c 00 6c 00 61 00 5f 00 64 00 69 00 5f 00 6c 00 61 00 76 00 6f 00 72 00 6f 00 00 00 46 6f 67 6c 69 6f 31 00 46 00 6f 00 67 00 6c 00 69 00 6f 00 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2979

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2979
Entropy:	4.43610309509
Base64 Encoded:	False
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 .
Data Raw:	cc 61 b5 00 00 03 00 ff 10 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 20 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 2019

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	2019
Entropy:	3.35046169998
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . Z . . . . . " . . . . . Q . . . . . K . v . . . J . . , . . | _ X . . . . .
Data Raw:	93 4b 2a b5 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 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 7e 02 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 268

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	268
Entropy:	1.7944240825
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . @ . . . . . ~ z . . . . . q . . . . . d d . . . . . i . . . . . w . . . . . a . . . . . z N . . .
Data Raw:	72 55 40 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 02 00 00 00 00 00 00 7e 7a 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 11 00 00 00 00 00 00 00 00 00 03 00 ff ff ff ff ff ff ff 06 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 2797

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	2797
Entropy:	1.97411509248
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . 8 . . . . . A . . . . . 7 . ` . . . q . . . . .
Data Raw:	72 55 00 02 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 38 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 03 00 d0 00 00 00 00 00 00 00 00 00 00 00 0e 00 0e 00 00 00 00 00 01 00 01 00 00 00 01 00 d1 03 00 00 00 00 00 00 00 00 00 11 08 00 00 00 00 00 00 00 00 41 08

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 1000

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	1000
Entropy:	2.49662055587
Base64 Encoded:	False
Data ASCII:	r U @ . . . . @ . . . . @ . . . . x . . . . . @ . . . . ` . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . O . x . . . . . . . . . . . . . . . ` . . . . P . F . O . @ . . . . ` . . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 78 00 00 00 08 00 40 00 e1 01 00 00 00 00 00 00 00 02 00 00 00 03 60 04 01 d9 08 ff 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_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 563

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	563
Entropy:	6.24783906376
Base64 Encoded:	True
Data ASCII:	. / . . . . 0 . J . . . . H . . H . . . . . . H . . . d . . . . V B A P r @ o j e c t . . . . T . @ . . . . . = . . . + . r . . . . y = . W c . . . . J < . . . . . . 9 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 . 0 . . . E O f f i c . E O . . f . . i . c . E . . . . E 2 D F 8 D
Data Raw:	01 2f b2 80 01 00 04 00 00 00 03 00 30 aa 4a 02 90 02 00 48 02 02 48 09 00 c0 12 14 06 48 03 00 01 64 e4 04 04 04 00 0a 00 84 56 42 41 50 72 40 6f 6a 65 63 74 05 00 1a 00 54 00 40 02 0a 06 02 0a 3d 02 0a 07 2b 02 72 01 14 08 06 12 09 02 12 79 3d a0 57 63 02 00 0c 02 4a 3c 02 0a 04 16 00 01 39 73 74 64 6f 6c 04 65 3e 02 19 73 00 74 00 64 00 00 6f 00 6c 00 65 00 0d 14 00 68 00 25 5e