

JOeSandbox Cloud BASIC



**ID:** 682695

**Sample Name:**

bergo.document.08.11.2022.doc

**Cookbook:**

defaultwindowsofficecookbook.jbs

**Time:** 20:51:46

**Date:** 11/08/2022

**Version:** 35.0.0 Citrine

# Table of Contents

Table of Contents	2
Windows Analysis Report bergo.document.08.11.2022.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	4
Sigma Signatures	4
Snort Signatures	4
Joe Sandbox Signatures	5
AV Detection	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
World Map of Contacted IPs	8
Public IPs	8
General Information	8
Warnings	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASNs	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\924A4EAB.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EF8F8D2.png	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E58F8177-9D22-4189-9792-5360446A7F20}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{570C9765-A79D-4233-901D-9E93C792BB62}.tmp	10
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{94DAC7F9-FA29-4FE8-9031-3C50514859C6}.tmp	11
C:\Users\user\AppData\Local\Temp\~DFED60CF98F04C552C.TMP	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\bergo.document.08.11.2022.LNK	11
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	12
C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm	12
C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	12
C:\Users\user\Desktop\~\$rgo.document.08.11.2022.doc	13
Static File Info	13
General	13
File Icon	13
Static OLE Info	13
General	13
OLE File "/opt/package/joesandbox/database/analysis/682695/sample/bergo.document.08.11.2022.doc"	13
Indicators	13
Streams with VBA	14
VBA File Name: ThisDocument.cls, Stream Size: 2868	14
General	14
VBA Code	14
Streams	14
Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 357	14
General	14
Stream Path: PROJECTwm, File Type: data, Stream Size: 41	14
General	14
Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7	14
General	14
Stream Path: VBA/_SRP_2, File Type: data, Stream Size: 5108	15
General	15
Stream Path: VBA/_SRP_3, File Type: data, Stream Size: 2724	15
General	15
Stream Path: VBA/dir, File Type: data, Stream Size: 486	15
General	15
Network Behavior	15
TCP Packets	15
Statistics	15

System Behavior

16

Analysis Process: WINWORD.EXEPID: 1932, Parent PID: 576

16

General

16

File Activities

16

File Created

16

File Deleted

16

File Read

16

Registry Activities

16

Key Created

16

Key Value Created

17

Key Value Modified

18

Disassembly

22

# Windows Analysis Report

bergo.document.08.11.2022.doc

## Overview

### General Information

Sample Name:	bergo.document.08.11.2022.doc
Analysis ID:	682695
MD5:	228c063e5ce747..
SHA1:	e13b37423003eb..
SHA256:	025d824f7fd0627..
Tags:	doc IcedID
Infos:	

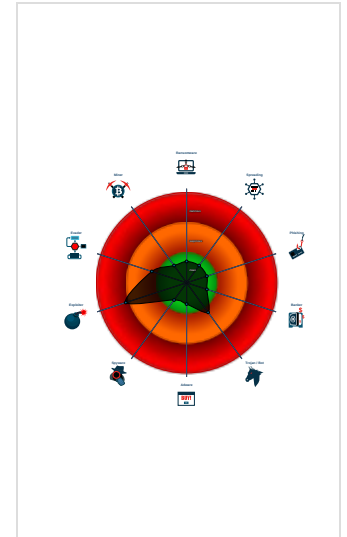
### Detection

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

### Signatures

Office document tries to convince v...
Multi AV Scanner detection for subm...
Document contains an embedded V...
Machine Learning detection for sam...
Potential document exploit detected...
Tries to connect to HTTP servers, b...
Document contains an embedded V...
Document contains embedded VBA...
IP address seen in connection with ...
Document misses a certain OLE str...

### Classification



## Process Tree

- System is w7x64
- WINWORD.EXE (PID: 1932 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- cleanup

## Malware Configuration

No configs have been found

## Yara Signatures

No yara matches

## Sigma Signatures

No Sigma rule has matched

## Snort Signatures

No Snort rule has matched

# Joe Sandbox Signatures

## AV Detection



Multi AV Scanner detection for submitted file

Machine Learning detection for sample

## System Summary



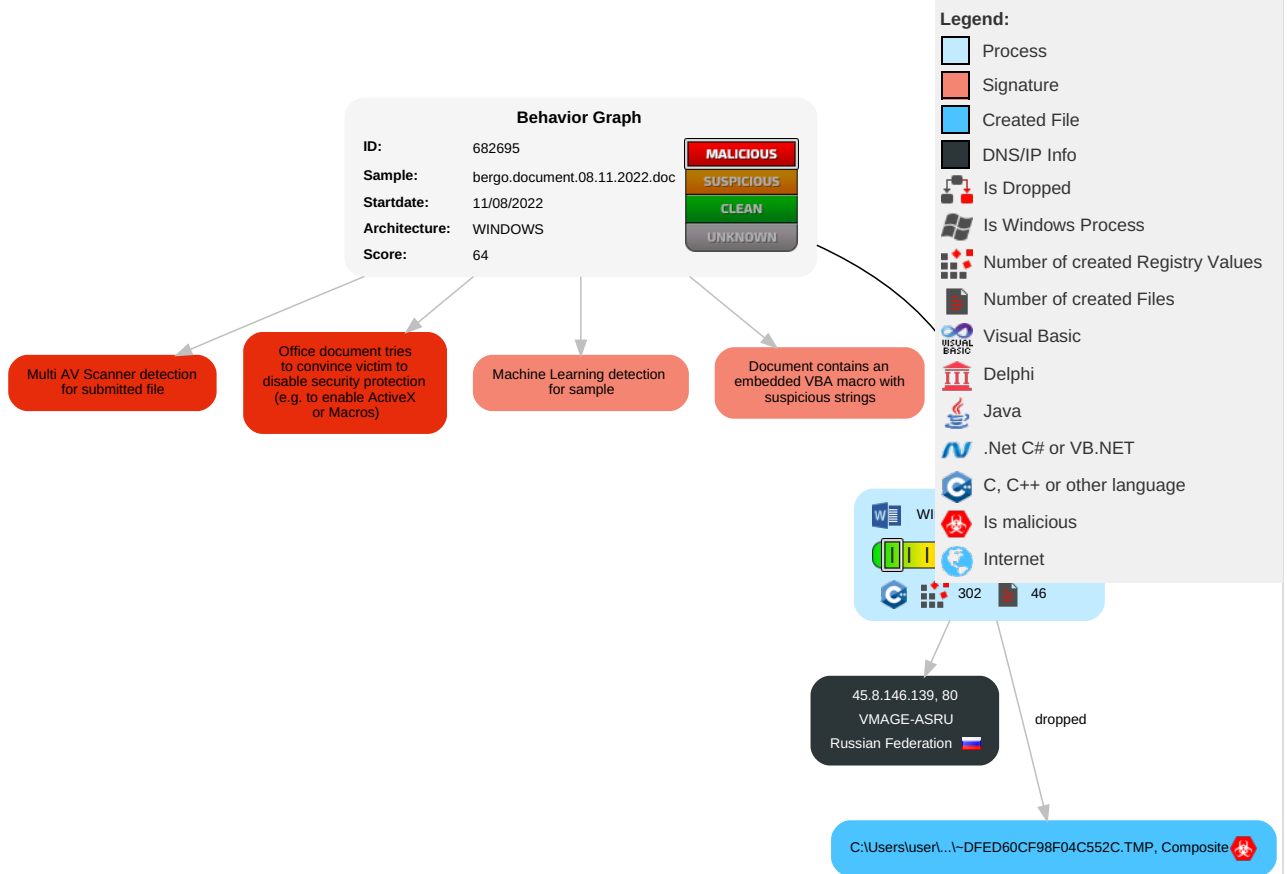
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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	Impact
Valid Accounts	1 2 Scripting	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 2 Scripting	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	Delete Device Data

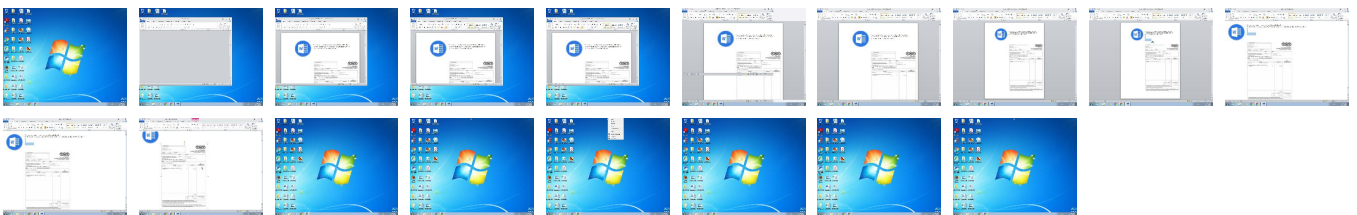
## Behavior Graph

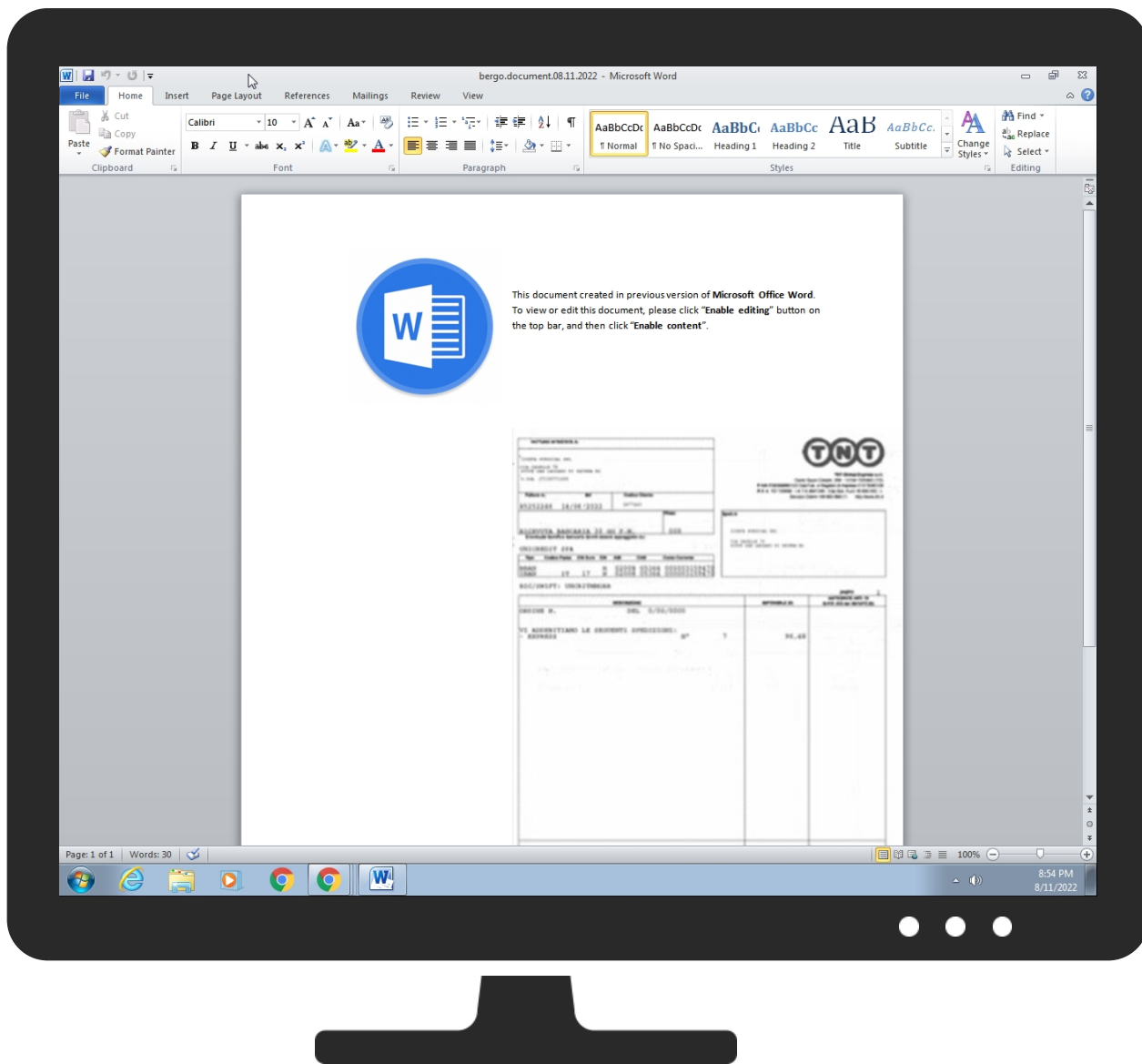


## Screenshots

### 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
bergo.document.08.11.2022.doc	25%	Virustotal		<a href="#">Browse</a>
bergo.document.08.11.2022.doc	18%	ReversingLabs	Script-Macro.Trojan.Amp hitryon	
bergo.document.08.11.2022.doc	100%	Joe Sandbox ML		

### Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DFED60CF98F04C552C.TMP	100%	Joe Sandbox ML		

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

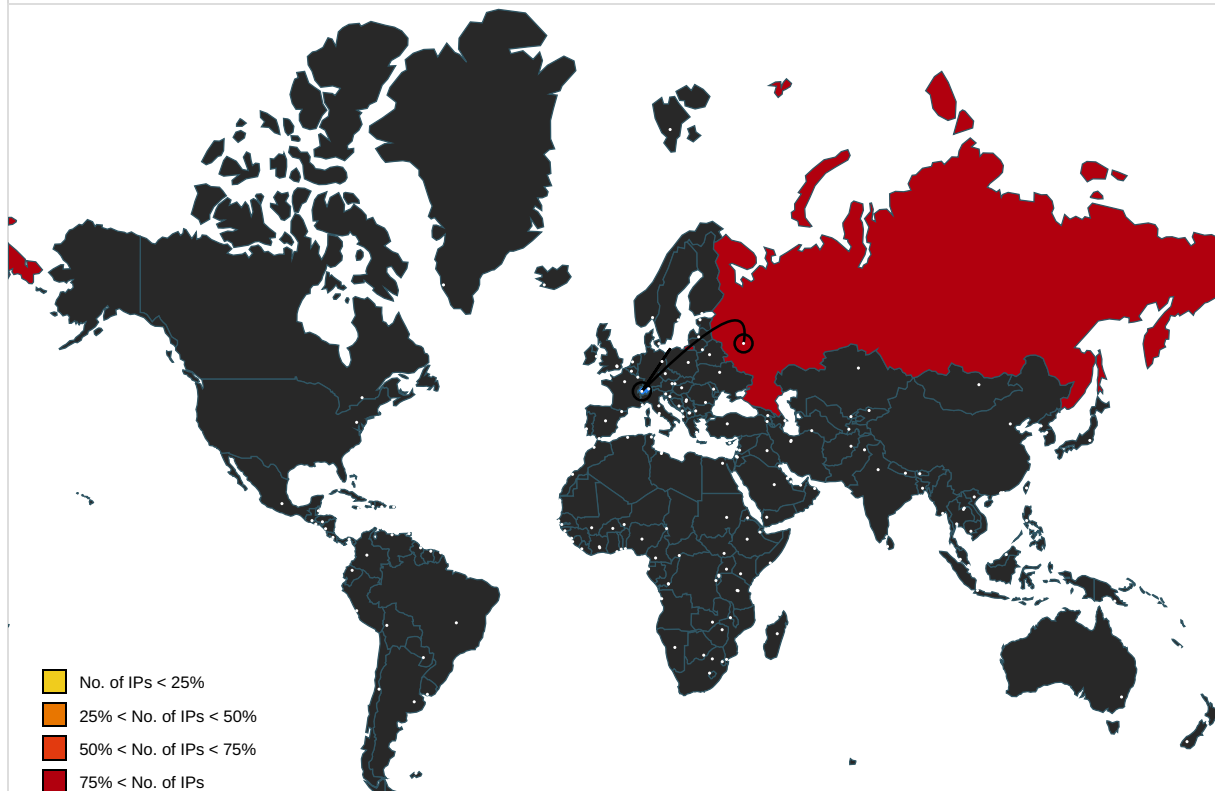
No Antivirus matches

## Domains and IPs

### Contacted Domains

No contacted domains info

### World Map of Contacted IPs



### Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.8.146.139	unknown	Russian Federation		44676	VMAGE-ASRU	false

## General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682695
Start date and time:	2022-08-11 20:51:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bergo.document.08.11.2022.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	4
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0



Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• GSI enabled (VBA)</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.winDOC@1/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li><li>• Number of executed functions: 0</li><li>• Number of non-executed functions: 0</li></ul>
Cookbook Comments:	<ul style="list-style-type: none"><li>• Found application associated with file extension: .doc</li><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found Word or Excel or PowerPoint or XPS Viewer</li><li>• Attach to Office via COM</li><li>• Scroll down</li><li>• Close Viewer</li></ul>

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\924A4EAB.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 380 x 526, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	79862
Entropy (8bit):	7.9850226558494
Encrypted:	false
SSDEEP:	1536:3oqyPqib6lbiXmcfDBFdEU8yslk2ZGBIGUCk4+:3yqtlmXmcbBFopLwIGDkH
MD5:	F673388F14A0B0E6160D7E31FB8B27A7
SHA1:	792480CA5B43D57E2A0A65466D77A294DA9D55C3
SHA-256:	0D79507FBC5D3C1843F0584E92FFD8B8F2862B4AE569BEB934963B30185E6489
SHA-512:	957C95FE8ED7DC213F027C59952F3F2AB5DFE6ED91944880D230AFC7B2B9EFFD812000FBF26CD6948DD3C478CB9B049C97405F6EBD4A86E3D10241DA3A0B652A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....4!.....IDATx...{#...9g...p...l+...^x..['.....9...g.K.t7.0#...Ca...S...[o.:N.:v.'.....r...W...q.....!.....q.CF.g..._c.y.....;9....6._Z.../.....nt../..g.t..._....._/-.....F.....+mt.X.../...+...0:...../..^.{...b.}`0.X...V...].8N0.\$..\....@0....l.ZqB.+?_...fR}...%.\....Y., A..r..Z..B~8..t.P.~.Cc[p.D.W.INn..f....5....c.If.V....Oh\$Y...]....Gl.....q... ..u..../.. ..b.`0.L.@ 0.L.@ (.....Ac..Rd...o.....6~x..v..t..._..Ph6.E"..... T..\_..p..e..1.o.....qf.uk/.km/w.Z.<...9.' >..B.PH....K.J.8...\$.; >g...A..3\.'_'_e....pX6x..(..m....Kc6...a.By;.P..R..M.u..p2. ....7..0V.kO..n...v#.. >.....pm....B.\$.-.h4:.N#.r..D" n<...ak..`0.k.g....d@q..Cf<wk..oW....5.....V.U.+.\$*...? 2..r..6...};=e.j.l)/....*...Y..t.L.....vG.H...tj.....`0..FL.H\$....d.P(..DB..j%....g.Y..<??o.Z...t....l.P(r.X,&k..._Fm>..Z....^ 7...).8.X.X,...t..Dd..{%.....y.8.x<...h6..H\$.H.\..` .O....(....B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EF8F8D2.png



Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 440 x 440, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	256277
Entropy (8bit):	7.980105068490826
Encrypted:	false
SSDEEP:	6144:lqua1wNXfdpQfqpdHWbjGadcQ4Lv8zhP9BXWZ:ZuaizWqpd0HdkyVBXu
MD5:	CF4AB970C74E474774B60BF03CFDC3CE
SHA1:	2E78C30BF4B9D673EECED99009F69FE8F525A06
SHA-256:	716D8319B106C690F8CD67E5611792FA7E7999FF0270CFE366DA3A02F815BE19
SHA-512:	1B7278E6ED4E548EA43B79483EDCEEA550AC0A73EC072577480AA07687CBA873BEBB1648303468323A24CEC8AE5C35ABC9F7B6C1440AFFE2E6A0660B57F10F91
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....7.....sRGB.....gAMA.....a.....pHYs..!.....IDATx^.....Eu.=..L.&.y..\$..h.....Dz.q..2F.4.....- A..h...\$.l...7..g..~.....u.N.u.O;.AuU.:uj.....9l....0 ..6..rm..O:.....J..^Y.Z.ICK~x...C.....[...6.. e... ..gZ..m.....;H..dez...[s...E.i...m.6/ E.i-Wn[f..N....Z..Z^i.i]5...e...+{...L...+0i.....C...5.HZ...w"y....3..TT..g..... /..o..m..z40K~. <..Kk.5.z..m:.q.4.i5.TZ....6~.%f..m.=...L.<...![[.1..D...x...*2....p....*oE.{E..}..p.....p]&mZ..e.@.k.5..9..W..j..-o..M...l..".oy*...o...{>..V...+...#z.DOH..K.<o.o&h.U.6..U.... WW.Syzh...+...i.H..IO\$-y@..6~K.....h.U...J...jZK...%2-[[.mZ.....2l...z<Pe..5..!<...7tP.=zMO.....g.....5=...D.'hm.Z.D..{..Z.....A/-i5.....hyZ\$-...g..S.T....."P.*j]...L.....OZ.3..8 ...<f...*...-O.g.....g.f..l.P...e.>+=6....[...%...%=Z.V.hy2....3.l.....=D.'...M..'*P. ....@.W.=.=...[c.^...2-].....A.3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{E58F8177-9D22-4189-9792-5360446A7F20}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.693156180267119
Encrypted:	false
SSDEEP:	192:hUKtjsCbo1FjwMf0vg/jbsSkantnzCbo1FjwMf0vg/jbsSka:ntYCbo1Jpc4/sSxtzCbo1Jpc4/sS
MD5:	B10B8C76994F98F2C5F2DFFB1A326AA0
SHA1:	9A8A1E46B450CA4241C6C1D435C75BB391796EEA
SHA-256:	B2B0137CF7AC08CFE6267C0985C0EFD3AABE30ED1199186D7AF880B16B9E2A65
SHA-512:	C6C2861A2D5BBD514884550F6BBD91ADA821D8045DE86A308320A7338C3426B3BFED69F7A321FAC1637AC662006F051B938EF2E62D295AE4E8E1D07EB962B66E
Malicious:	false
Reputation:	low
Preview:	.....>..... ..... ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{570C9765-A79D-4233-901D-9E93C792BB62}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCEDE5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..... ..... ..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{94DAC7F9-FA29-4FE8-9031-3C50514859C6}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	2.123533094102747
Encrypted:	false
SSDEEP:	12:DMlzfRLZRW4WZ1MFKuQ9cc3xn82ISkwkvS4vW4tW4PllgWHkUZZ/W4c:4LG1ND9Pxn824k0aWOWYCWHz
MD5:	89F597A15C87E50517A7A280CD3EBC3C
SHA1:	82939B3762B83F9F7605BE0934BB8BB8BB8E2FA0
SHA-256:	231CDA131C5AD56C80BC94AF08CD13B596D4565A065A405AEF2B34B65840613F
SHA-512:	C7B121899682AB4500BA13F2814C5A4B26B314B6199EDB23CE975C4436FFA4FB8066266C5F6B35969D16F9D62BECBED166218E929D1FF714886F6613A0D8B90E
Malicious:	false
Reputation:	low
Preview:	...T.h.i.s .d.o.c.u.m.e.n.t .c.r.e.a.t.e.d .i.n .p.r.e.v.i.o.u.s .v.e.r.s.i.o.n .o.f .M.i.c.r.o.s.o.f.t .O.f.f.i.c.e .W.o.r.d....T.o .v.i.e.w .o.r .e.d.i.t .t.h.i.s .d.o.c.u.m.e.n.t., .p.l.e.a.s.e .c.l.i.c.k . .E.n.a.b.l.e .e.d.i.t.i.n.g. .b.u.t.t.o.n .o.n .t.h.e .t.o.p .b.a.r., .a.n.d .t.h.e.n .c.l.i.c.k . .E.n.a.b.l.e .c.o.n.t.e.n.t. .... .....Z..... ..... .....

C:\Users\user\AppData\Local\Temp\~DFED60CF98F04C552C.TMP  	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	60416
Entropy (8bit):	4.170879206129513
Encrypted:	false
SSDEEP:	768:h2U1g/IoQP1Avvsyd9OSlbqtANjXJj3BnjeGZkwx5qxwGAacg:h8IoQPev9d9OSletAr0Ghx5qSGAacg
MD5:	D59E78BA006DCA8FC03E6986D29BDB76
SHA1:	4483ADAFAD9F7FD9474079E0A8D69FD840693815
SHA-256:	37A32C87A0EA8D4769D7C4F2B04A8FA900FD917676A7C023DAB4068B834BB475
SHA-512:	699D4875F4DB7B08AE9477D03BB653BC707182CEAC2C05640FAAFD98A2940B891A764561D5969842EE80DD8F362F4ECDB4F1B7A9959605D9FB857160BD8FF25
Malicious:	true
Antivirus:	<ul style="list-style-type: none"><li>Antivirus: Joe Sandbox ML, Detection: 100%</li></ul>
Reputation:	low
Preview:	.....>..... .....T.....( .....!.."#..\$..%..& . '.....)*...+...-...../..0...1...2...3...4...5...6...7...8...9...<...=...>...?...@...!..B...C...D... ..E...F...G...H...;...J...K...L...M...N...O...P...Q...R...S.....`...V...W...X...Y...Z...].\..... ..._.....b...c...d...e...f...g...h...[...j...k...t...m...n...o...p...q...r...s...^.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\bergo.document.08.11.2022.LNK
---

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:52 2022, mtime=Tue Mar 8 15:45:52 2022, atime=Fri Aug 12 02:53:11 2022, length=2221899, window=hide
Category:	dropped
Size (bytes):	1089
Entropy (8bit):	4.559362124859331
Encrypted:	false
SSDEEP:	12:8hCTCm\vgXg\XAICPCHaXRBktB\eLX+WufkW\xgiTc4icbv9\I4EIDtZ3YiIMM5:8h+h\XThOMY8W\xforeT9\l6Dv3qdu7D
MD5:	003043F3F1B9D24A4EC9757C82A5E63C
SHA1:	1E981BCE6BD5AD9C631E7513382249481546684B
SHA-256:	D6F110658A1FCC45AA044F5C53025BBF8D41788C1F5CB3361EF108DC6621509A
SHA-512:	463BCDD1A0D1FFB4218176DCF7502D22EE7D1B4E997A039E2F88EBFAF0774442D8BEA56E9B0F61FF81F3BBD8E012CA513650F4E8DEF1198A2F25FD80C8F7C970
Malicious:	false
Reputation:	low
Preview:	L.....F.....\$.3.....\$.3.....K!......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.....hT....user.8.....QK.XhT.*...&=...U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT.*..._.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.6.9.....2.K!.!..U.. .BERGOD~1.DOC.h.....hT..hT.*...r....'. .....b.e.r.g.o...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....-...8...[.....?J.....C:\Users\..#\.....\\367706\Users.user\Desktop\bergo.document.08.11.2022.doc.4.....\.....\.....\.....\D.e.s.k.t.o.p\..b.e.r.g.o...d.o.c.u.m.e.n.t...0.8...1.1...2.0.2.2...d.o.c.....,LB.)...Ag.....1SPS.XF.L8C....&.m.m.....S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X..

<b>C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.642026852171083
Encrypted:	false
SSDEEP:	3:bDuMJlfyF8oALRlj9omX1xQ8oALRlj9ov:bCUyFtAlr9itAlr9y
MD5:	B2F218041B0F211C03F9CDAD574B84F9
SHA1:	24EAA43E1E915A6459650FBC65DCE94339079CC1
SHA-256:	EB84EE53E0ABF646203578F381883080960072CFE3F0462A3FBD7BB7EE36D66B
SHA-512:	1C8B4DF8649F493B35FD4B8EE262FBB28904B43F6F20A081E59110EDF2CA0C34E72770B874D91487FD92A7495A241AACB838924C337D449329842BA6F5DF22A3
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..bergo.document.08.11.2022.LNK=0..[doc]..bergo.document.08.11.2022.LNK=0..

<b>C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/lN:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AF A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....X...

<b>C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false

SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

<b>C:\Users\user\Desktop\~\$rgo.document.08.11.2022.doc</b>	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJyIp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/I
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AFA
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

<b>Static File Info</b>	
<b>General</b>	
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.99348706678991
TrID:	<ul style="list-style-type: none"><li>Word Microsoft Office Open XML Format document (49504/1) 49.01%</li><li>Word Microsoft Office Open XML Format document (43504/1) 43.07%</li><li>ZIP compressed archive (8000/1) 7.92%</li></ul>
File name:	bergo.document.08.11.2022.doc
File size:	2316883
MD5:	228c063e5ce747dd51ffbdf31dcc1f9
SHA1:	e13b37423003ebf1aacc898435607dc471ae0bd6
SHA256:	025d824f7fd062715efe4914065eb6026a0f1720256f03e18c652978ec9d6844
SHA512:	0f6c3c0f467c1d6f6b8915fd93a9034ea87bddc4b95225c444cd48f2f735f2e09b379febf2951b7ce76ceee9f61191f61bcf6c299d28f974825e6e425ee2159a
SSDEEP:	49152:FNbf0FGXHT9mAtoLOXOx1dPtHdSBEPd2rB9:F5f0F2HECAndXKEM
TLSH:	CCB533BF0CC46EF4D6A7C931261C30AE5C9361925D0E5B6EF1F1DB0AD668C8D0DA198B
File Content Preview:	PK.....!.U~....._rels/.rels...J.@.....4.E..D.....\$....T..w-.j..... .zs..z..z.*X.%(v.....6O.{PI.....`S__x.C..CR.....t.R.....hl.3..H.Q..*.;..=..y... n.....yo.....[vrf..A..6..3[>_...K.....\NH!.....<.r...E.B..P...<_.

<b>File Icon</b>	
	
Icon Hash:	e4eea2aaa4b4b4a4

<b>Static OLE Info</b>	
<b>General</b>	
Document Type:	OpenXML
Number of OLE Files:	1

<b>OLE File "/opt/package/joesandbox/database/analysis/682695/sample/bergo.document.08.11.2022.doc"</b>	
<b>Indicators</b>	
Has Summary Info:	

Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	True

<b>Streams with VBA</b>	
<b>VBA File Name: ThisDocument.cls, Stream Size: 2868</b>	
<b>General</b>	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	2868
Data ASCII:	..Attribute VB_Name = "ThisDocument"...Bas..1Normal...VGlobal!.Spac.IfFalse.JCreatabl..Pre declare..Id..#True."Expose..TemplateDeriv.\$CustomlizC.P....D.? PtrSafe Function .....Lib "user.32" Alias "KillTimer" (ByVal ..... As Long.0, .....)..
Data Raw:	01 87 b4 00 41 74 74 72 69 62 75 74 00 65 20 56 42 5f 4e 61 6d 00 65 20 3d 20 22 54 68 69 00 73 44 6f 63 75 6d 65 6e 10 74 22 0d 0a 0a 8c 42 61 73 01 02 8c 31 4e 6f 72 6d 61 6c 02 2e 19 56 47 6c 6f 62 61 6c 21 01 aa 53 70 61 63 01 6c 46 61 08 6c 73 65 0c 4a 43 72 65 61 10 74 61 62 6c 15 1f 50 72 65 20 64 65 63 6c 61 00 06 49 64 11 00 23 54 72 75 0d 22 45 78 70 08 6f 73 65 14 1c 54

<b>VBA Code</b>	

<b>Streams</b>	
<b>Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 357</b>	
<b>General</b>	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	357
Entropy:	5.292924656590583
Base64 Encoded:	True
Data ASCII:	ID="{0DA1E065-B0B9-45A3-A487-E3C98DDC0182}"..Document=ThisDocument/&H00000000..Name="Project"..HelpContextID="0"..VersionCompatible32="393222000"..CMG="181AF8FEF8FEF8FEF8FEF8FE"..DPB="3032D215D315D315"..GC="484AAA2DAB2DABD2"....[Host Extender Info]..&H000000
Data Raw:	49 44 3d 22 7b 30 44 41 31 45 30 36 35 2d 42 30 42 39 2d 34 35 41 33 2d 41 34 38 37 2d 45 33 43 39 38 44 44 43 30 31 38 32 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

<b>Stream Path: PROJECTwm, File Type: data, Stream Size: 41</b>	
<b>General</b>	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.0773844850752607
Base64 Encoded:	False
Data ASCII:	ThisDocument.T.h.i.s.D.o.c.u.m.e.n.t.....
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

<b>Stream Path: VBA/_VBA_PROJECT, File Type: ISO-8859 text, with no line terminators, Stream Size: 7</b>	
<b>General</b>	
Stream Path:	VBA/_VBA_PROJECT
File Type:	ISO-8859 text, with no line terminators
Stream Size:	7
Entropy:	1.8423709931771088
Base64 Encoded:	False
Data ASCII:	a . . .
Data Raw:	cc 61 ff ff 00 00 00



# System Behavior

**Analysis Process: WINWORD.EXE**    PID: 1932, Parent PID: 576

## General

Target ID:	0
Start time:	20:53:12
Start date:	11/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fe50000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

## File Activities

### File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory   synchronize	device	directory file   synchronous io non alert   open for backup ident   open reparse point	success or wait	1	6E102B14	CreateDirectoryA

### File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\--DFED60CF98F04C552C.TMP	success or wait	1	6E180648	unknown
C:\Users\user\Desktop\~\$rgo.document.08.11.2022.doc	success or wait	1	6E180648	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
---------------	---------------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

### File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Fonts\StaticCache.dat	unknown	60	success or wait	1	6E47A0EB	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	1	success or wait	1	6E071925	unknown
C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	unknown	4096	success or wait	1	6E071925	unknown
C:\Users\user\Desktop\bergo.document.08.11.2022.doc	1872093	184	success or wait	2	6E180648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9EF8F8D2.png	0	65536	success or wait	4	6E180648	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\924A4EAB.png	0	65536	success or wait	2	6E180648	unknown

## Registry Activities

### Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6E15A5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6E180648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6E180648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6E180648	unknown














Disassembly

 No disassembly