ID: 432926
Sample Name: document-47-2637.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 23:33:10
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

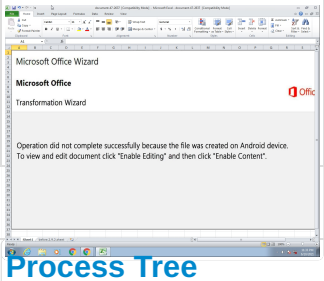
Analysis Report document-47-2637.xls

Overview

General Information

Sample Name:	document-47-2637.xls
Analysis ID:	432926
MD5:	92dcc47a1a044fc..
SHA1:	6f9266a6c0b702c..
SHA256:	ac4b99079b1ceb..
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

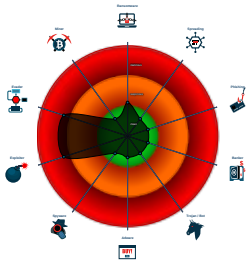
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Allocates memory within range whic…
- Dropped file seen in connection with…
- Drops PE files
- Extensive use of GetProcAddress (o…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1204 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2668 cmdline: 'C:\Windows\System32\cmd.exe' /c copy '%ProgramFiles(x86)%\Internet Explorer\ExtExport.exe' C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - nnAzot.exe (PID: 2628 cmdline: 'C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe' C:\aZ8ThU0Y\ERdZMUem GdPT AuMr7 MD5: 7F7F391491C315A4A72EFCAC0D34FA93)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

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 submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

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

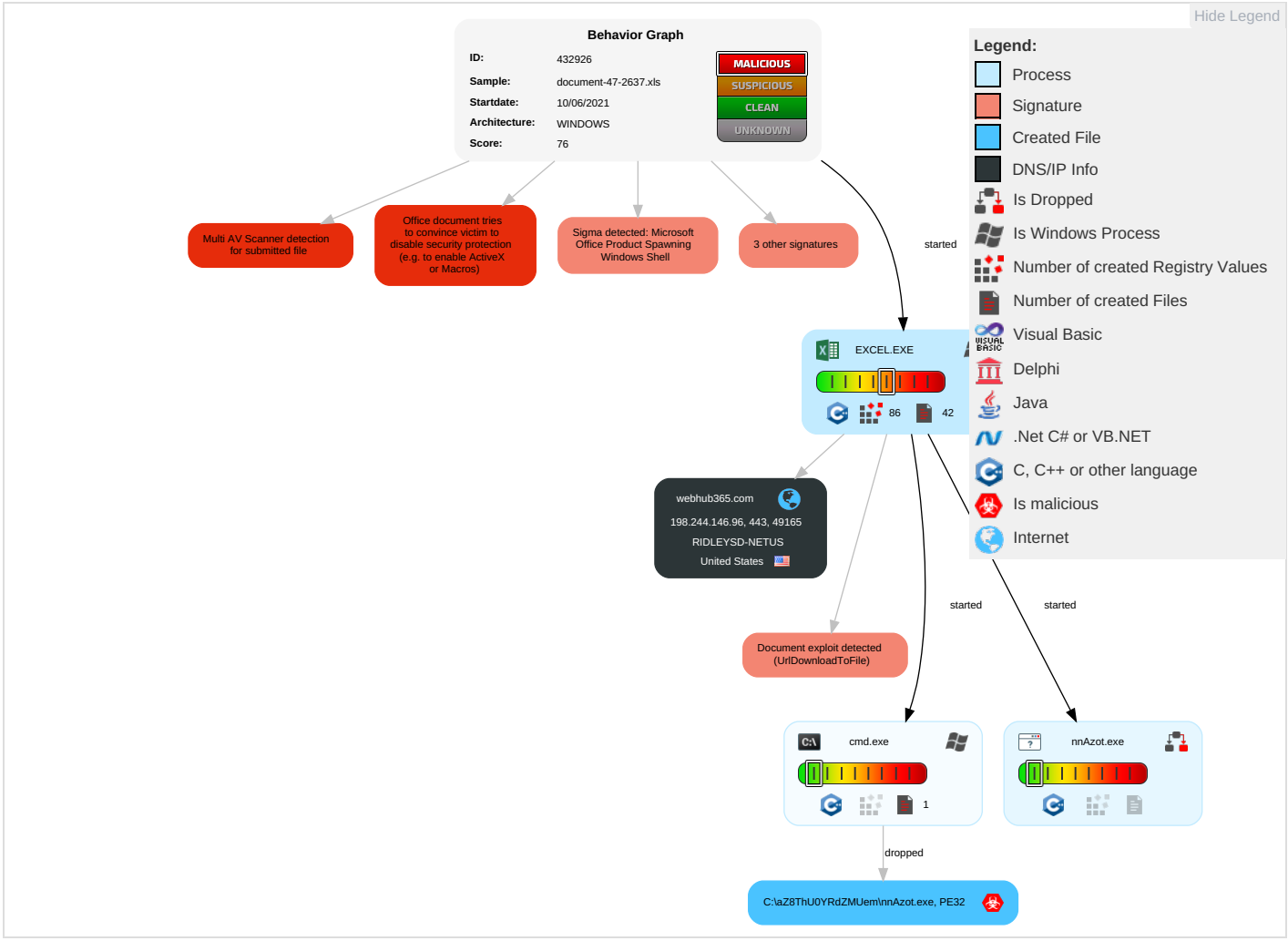
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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
Valid Accounts	Command and Scripting Interpreter 1	Application Shimming 1	Process Injection 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	Application Shimming 1	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	Exploitation for Client Execution 2 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

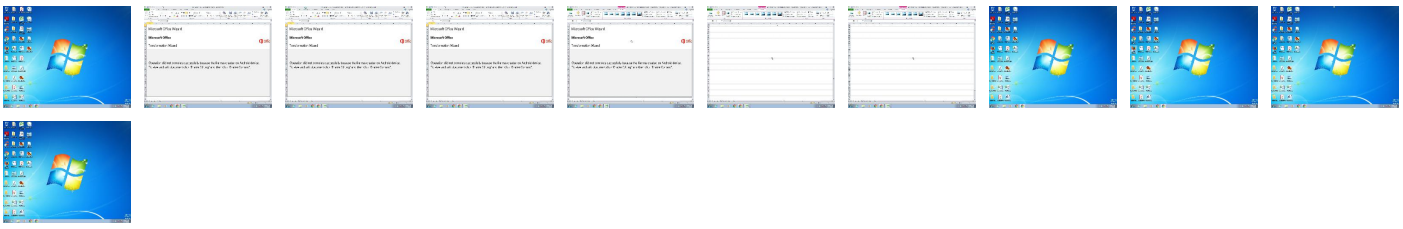
Behavior Graph

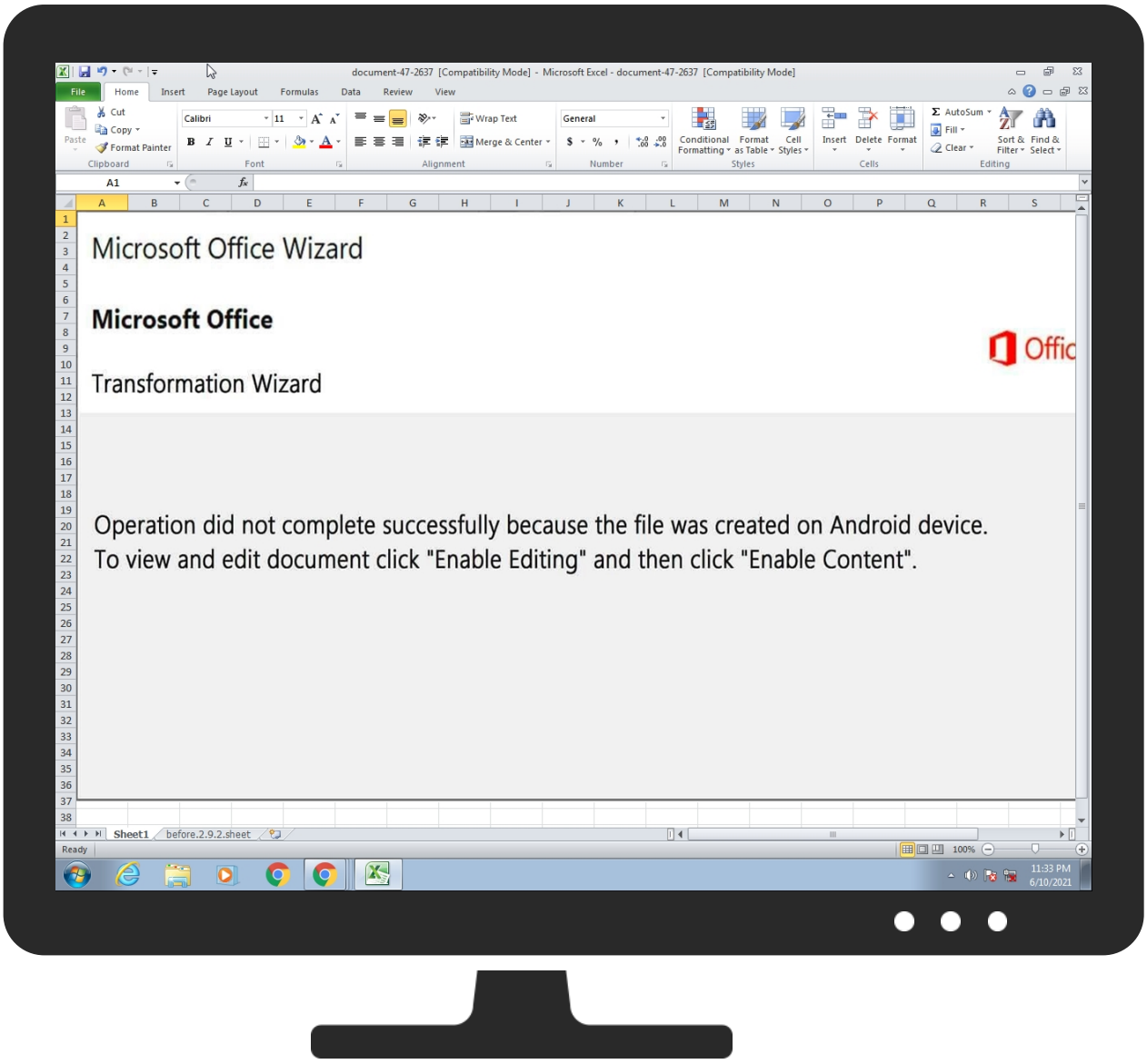


Screenshots

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
document-47-2637.xls	26%	Virustotal		Browse
document-47-2637.xls	23%	Metadefender		Browse
document-47-2637.xls	15%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	0%	Virustotal		Browse
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	2%	Metadefender		Browse
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
webhub365.com	0%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webhub365.com	198.244.146.96	true	false	• 0%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.244.146.96	webhub365.com	United States		18630	RIDLEYSD-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432926
Start date:	10.06.2021
Start time:	23:33:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-47-2637.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
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:	mal76.expl.evad.winXLS@5/14@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 88.6%) • Quality average: 72.2% • Quality standard deviation: 34.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	ManyToOneMailMerge Ver 18.2.dotm	Get hash	malicious	Browse	• 198.244.146.96
	WV Northern Community College.docx	Get hash	malicious	Browse	• 198.244.146.96
	Tax Folder.doc	Get hash	malicious	Browse	• 198.244.146.96
	51564.docx	Get hash	malicious	Browse	• 198.244.146.96
	f.xls	Get hash	malicious	Browse	• 198.244.146.96
	P.I-84514.doc	Get hash	malicious	Browse	• 198.244.146.96
	P.I-84512.doc	Get hash	malicious	Browse	• 198.244.146.96
	swift_euro.docx	Get hash	malicious	Browse	• 198.244.146.96
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 198.244.146.96
	Y8bVoElk4Y.xls	Get hash	malicious	Browse	• 198.244.146.96
	xTnb7uPpSb.xls	Get hash	malicious	Browse	• 198.244.146.96
	statistic-608048546.xls	Get hash	malicious	Browse	• 198.244.146.96
	212161C3EFE82736FA483FC9E168CE71#U007eC2 #U007e1B6B2C73#U007e00#U007e1.xlsx	Get hash	malicious	Browse	• 198.244.146.96
	cryptowall.exe	Get hash	malicious	Browse	• 198.244.146.96
	invoice-H9247.docx	Get hash	malicious	Browse	• 198.244.146.96
	T3ZhUk5pyO.xls	Get hash	malicious	Browse	• 198.244.146.96
	Invoice.xlsm	Get hash	malicious	Browse	• 198.244.146.96
	Prudential Investment Services.doc	Get hash	malicious	Browse	• 198.244.146.96
	Donation Receipt 36561536.doc	Get hash	malicious	Browse	• 198.244.146.96
	cryptowall.exe	Get hash	malicious	Browse	• 198.244.146.96

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	document-37-1849.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j._iK..|[.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vI..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.l..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?!I..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....].....B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.114179942967892
Encrypted:	false
SSDEEP:	6:kKXF6e8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:M8kPlE99SNxAhUe3OMx
MD5:	2E7776A8352D7B7340867AA27A128846
SHA1:	FD6DA9992DCEE317941DE8A460F26EBB4FEB94BD
SHA-256:	C708CF029849616022F4F6F176AB59DF8DE3A5AB0E31DBA7B081338001474C41
SHA-512:	0F9164C48E115C7180724B1BCBC52D711E83B17C9E448B8839B5639583BF948EBA0DF9E28B46518CA93488A30E1637C80DA046D5982BF4B31D27150E467DF364
Malicious:	false
Reputation:	low
Preview:	p..... .....Frh..^..(..... .....L.....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b..."..0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.035850934668823
Encrypted:	false
SSDEEP:	3:kkFklXQHlXfllXlE/JADkdllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yWJ/f/:kKXFGADk5liBAIdQZV7QWB
MD5:	221EE22598CAC868C8B16EE6D78B76D1
SHA1:	EEF00367633C5F7FAF69428C39C9107DEB332533

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
SHA-256:	D0B5F4D8A653A322B01BDF32CB6573DBEFFD78527CEB7BFDA518855D69CB4F79
SHA-512:	8E771B8C3BF7AAA920B177C435979C6947231ABF84654209FD17793ADA0391A52ADF3918F1E01AC37E58945BBD91489CA734F35F22E280A6A2E394320DF3AE34
Malicious:	false
Reputation:	low
Preview:	p..... ....`...~.*..^..(..... .....e..S.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.c.3.6.7.2.e.8.3.f.1.4.0."...

C:\Users\user\AppData\Local\Temp\57CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	68561
Entropy (8bit):	7.608965484613486
Encrypted:	false
SSDEEP:	1536:m+yXkNLPHqvAk/Vi6+YDT7Hbc8hxCCV2D:m+yUNLP4lA6+YHcId2D
MD5:	E7F218C4D29FEBD5A30BB644B9DE75EC
SHA1:	B32B0BFA6E62EFC6CF9265142A0CC837E73FAE06
SHA-256:	578A9F819A33168A169E9B01383EA68D40B526B1BEB9C16E9C711D75436B73DB
SHA-512:	DD82863199BB14A0F8BFE15E2D25C9362DF62CF3B2D46453FAF2C10FC2B12DE1890031479867E20655896D1F96FD384FA4F80D1605F1A4E2D0EFD96057D20B4
Malicious:	false
Reputation:	low
Preview:	.TKo.0.....0t-l.=.....>.].u?...X.^..6....4k. ^.^l... %rz.r.y.D&.^.w..WA.....h(..`..^......"5...!..CJR.:..D..... .gZ..j.....7....s....M.q.O677+..q.'.B4W..E.....1.-.a Fk.d.N>{.....Y. .`"..uqX.D.z+....r&.....u...%..c...8Iq..B...;.*.....9..:<.T.$...?$..Y..s.P.....:..AW2g..I]....O5....zD&.CY.....R^[.O..tLy...WN..n.-.....X.....%:...>.H<>..^..^/.62..lp..zi..]~..^.a.n...mY. ../.....PK.....!...<.....[Content_Types].xml ...(..... ....N.0...H.C...nH....

C:\Users\user\AppData\Local\Temp\CabCFBF.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j._iK..|||.w.M.!<-.}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K.....3.9.I..`D..e.i`....y...,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\Local\Temp\TarCFC0.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	156885
Entropy (8bit):	6.30972017530066
Encrypted:	false
SSDEEP:	1536:NlR6c79JjgCyrYBWsWimp4Ydm6Caku2SWsz0OD8reJgMnl3XlMuGmO:N2UJcCyZfdmoku2SL3kMnBGuzO
MD5:	9BE376D85B319264740EF583F548B72A
SHA1:	6C6416CBC51AAC89A21A529695A8FCD3AD5E6B85
SHA-256:	07FDF8BC502E6BB4CF6AE214694F45C54A53228FC2002B2F17C9A2EF64EB76F6
SHA-512:	8AFC5D0D046E8B410EC1D29E2E16FB00CD92F8822D678AA0EE2A57098E05F2A0E165858347F035AE593B62BF195802CB6F9A5F92670041E1828669987CEEC7DE
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Temp\TarCFC0.tmp	
Preview:	0..d...*.H.....d.0..d....1.0...`.H.e.....0..T...+.....7.....T.0..T.0...+.....7.....L.E*u...2105191915O3Z0...+.....0..T.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00. .+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Fri Jun 11 05:33:36 2021, atime=Fri Jun 11 05:33:36 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.4783997226177314
Encrypted:	false
SSDEEP:	12:85QvLgXg/XAlCPCHaXgzB8IB/64YvX+WnicvbZ1ObDtZ3YilMMEpxRljKoTdJP9O:85l/XTwz6IzYvYe11CDv3qtrNru/
MD5:	DDDE4AEA52639A376DDEA0363A830989
SHA1:	42C60E4DB7ACC6484B7F49E04B85E1F50B0939C8
SHA-256:	1C26913AC092AFA7B73B276E5BA1C121F6BDC6C67FE1FB4E7DDA837CA5BBDA63
SHA-512:	F5EAED45DEE831251AF7DD6993A01C76336E306D9C58792880C7FD833D36572E45C82516DC1FEA4C993915191D3540778EAAD65209BC0251FC3249423FB8F75A
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G..C.>..^..C.>..^...0.....i....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....R34..Desktop.d.....QK.X.R34*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\960781\Users.user\Desktop.....\.....\.....\.....\.....\D.e.s.k.t.o.p.....:.,.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.....960781.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-47-2637.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:12 2020, mtime=Fri Jun 11 05:33:36 2021, atime=Fri Jun 11 05:33:36 2021, length=92672, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.5358356147395575
Encrypted:	false
SSDEEP:	24:8u/7/XTwz6I4U8HMe11n1Dv3qtdM7dD2u/7/XTwz6I4U8HMe11n1Dv3qtdM7dV:8Q/XT3InaMWEtQh2Q/XT3InaMWEtQ/
MD5:	F5F66094ECB1402555729E1107D3C096
SHA1:	38CCFCC00261AFF0B8F487E60F8DB2215979FF9A
SHA-256:	A93527F892D71FDD7A251FEC2150DB068424F7EC190FC4416EC463E90BCE164E
SHA-512:	EE75541A6EC71E5F19138B342773FF6DF87264EDE25F6E5961CAA9BF3EB0B55F28AA75BDFEF20E34BA69D64EEF865AF3541A1A8D01C1237E2765572C319D369F
Malicious:	false
Preview:	L.....F.... ...E....{..C.>..^....C..^...j.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....r.2..h...R/4 .DOCUME~1.XLS..V.....Q.y.Q.y*...8.....d.o.c.u.m.e.n.t.-.4.7.-.2.6.3.7...x.l.s.....~.....-...8...[.....?J.....C:\Users\..#.....\\960781\Users.user\Desktop\document-47-2637.xls.+.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.4.7.-.2.6.3.7...x.l.s.....:.,.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.....960781.....D_....3N...W...9F.C....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.781102818999889
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRkKSd6YCZELRkKSd6YCmMY9LRkKSd6YCv:dj6Y9LaJdzgELaJdzUY9LaJdzs
MD5:	CC574425794FB97F59C2DC249939493A
SHA1:	8CA2DFD4C2535E0FFEB160319D2CD079758B7F8D
SHA-256:	1D977854F9C0DDF7462B6991CA2B6026C4FFCAF52F158A2C7B81B8FBEE5E35F0
SHA-512:	6C9C7CAFA742354DB174653D4C1CF9521AC10C67177FB2E26A85AE1267F1A45094BD1F1AE3C0B53836D5210F6083906F17C26A28A197D0CCF2F76D7447272E43
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..document-47-2637.LNK=0..document-47-2637.LNK=0..[xls]..document-47-2637.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WX9VC4P4.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WX9VC4P4.txt	
Category:	downloaded
Size (bytes):	99
Entropy (8bit):	4.712733418867265
Encrypted:	false
SSDEEP:	3:12EwDIJJaOXvzSGTKvUQ2VVvWYd6SsUFvWsUTR:8r9gzSGZX/vWYcSsOvTe
MD5:	BD6147C9030F0D655787BE45213DB496
SHA1:	BEEDCBABD678F5969FA7BB2012CB25BB8FCB4CF5
SHA-256:	5CAAF34D2E2E45E1677E131C8C64D202EF39B7D9B235C6E4165DB2EC87E7B4DB
SHA-512:	BC47F84968B6609AE4491B17B5C4FB074795ED6730E93C6A6A0E54CB31AF454123582A1BBCD11265E6D52592A40DE0BDF794A6660D77193E0CAA21BB8735AD5E
Malicious:	false
IE Cache URL:	webhub365.com/
Preview:	PHPSESSID.j12bufirjllllavl516k1pa431.webhub365.com/.1536.2129936640.30891785.3065758319.30891659.*.

C:\Users\user\Desktop\18CE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	117436
Entropy (8bit):	7.92560369680784
Encrypted:	false
SSDEEP:	3072:J2KY73qo5oIYZObwnLPdVSudf2azHqMf2azC2KY7A:J2ZouyzWuDzKizC2ZM
MD5:	0A6CFFEA7C8A3F28DB32D6B10FB143FF
SHA1:	D1565F223B143944C30884D301B52AD4E32EE47B
SHA-256:	FD7BDC282938F884B95DDAC7AC1EA44E18DB8664D063962A534FD61B03CC00BC
SHA-512:	C74DA35C7C0179207B9D20027F65524B87DED1063493F3FC87023737180E3B919AA1613E973FB876304BBBC57DA43298234E585CE4B09616D63DD20A70A04601
Malicious:	false
Preview:	........g2........../..........z7.;K/.....-..QE<...j.....!...4...k...A.....g2........./.6.....z7.;K/.....-..QE<...j.....!...4...k...A.....\.p.....xFU..p..&....Z.(u.E.,..T...eHcPU...r.....;j;..=....u7.Oo...0.8D..?.R.&..n}.#a.....L..u....n.B.....a.....=.....o.....\.....=.....9...!- .r.....@.....:k".....l.....+1...~.. 5A.....b0....V..e..".1.....:1..8&..B..3..esQ.&$..w..-1....X..>.M2..S.....#R...'.1.....(.z%...`.....w.Kt.H..D.hac1.....K..yO.....&q..2k^KQ.#....3.21.*.rp.....R.y$t.*.5.$K.....i>.VA....LG..g.1....f....[-C'y?....$..iv..:k.1.1.....J..i.u..v....n.<.....)...1.....~.X..&...d...#d.oj..qm.;#1...*...u.k..DI.NL..O.....g....1....?..i..U..m..i..m.d.K)0.f.67z1...-P.f.D....y..tE.BNc.....~.dK.1...&.. %.x]...y..+..2..o....D....1...N....z.@.....+..h...^nQ..F..`1...t.B.....D~.y.?.:.J.-.....".;.1.....N.k.}.*.P.\..c.C.....1...;....>.cv+Z.$..Xc..n..V*L..;..1...

C:\Users\user\Desktop\D73F0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	modified
Size (bytes):	99731
Entropy (8bit):	7.930414704009687
Encrypted:	false
SSDEEP:	1536:OGEtPTbpH0zoWOYUoFJTU1T8HdYtJEv0W0GEtPTbo:OvXpH0TUo5HdZR0vXo
MD5:	6D8E6965F252B13FF8D880053C83D123
SHA1:	47B7D1032C44D1D914B378F37492E17B0D7A2E59
SHA-256:	67D293F9AC0E32D54F1632FCCC7221DDB84E27D0278A5F403E81BB2A09CAEC0B
SHA-512:	5E485E8DE74B6D1D17C3028A5526ECDC7ED342A6C775FD2C48DBBF914FD034841D7F8DFF3DEE735C401A5B5A1CFA6B4DE2543BE4AF2E2C8EB84DF6C1EB37CD5
Malicious:	false
Preview:	........g2........../.........G....@...Jl.....D...)%.....i?....+.|U0..._.....g2........./.6.....G....@...Jl.....D...)%.....i?....+.|U0..._.....\.p..w....J.k1...O...6.`.....6.....gR..x.Kpk.Yz..y.....V.j.....o.L.|'.zQ...-..74..T.....l.(A...B.....a.....=...K.s.....!.....W|.....3.....=.....(.....i)B.P.@.....H."....t.....i1.....X.+.{.E...#>..;zb.+..(p..`1..d...ngwEm.h.Z#...s.H>.....1...}.oO.^.p~.....;t..OS.....nk1....!.A.h..O.F..=...u...q..op...1.....xp..K.@!.....%.Df..a1.*..-.u...[.....^...).p..:H..l...i0.j`...1...iY.....[.;.OP..p...'.....`1....j|..m.g.e2.1dl5>..pgq"W...:91...RI.@..NI..."....*R.....$P..,1....y.E._...lz.....yq..Y..(.!.1...F.0..M.OH.....{....RF:.|..u..1...f.....%-T3\.F...^.a.o]%{...1...l..IKl....b"EeN.i..Z.G.....D1....p.}.Q1E.k..^.J!.h.F%.X...8.1...M[}..@....P...`,.BS...).}_+.1.....cJ>R!.U?.L.=.X!.M...f..1....n-!.../...0.....Q.T.....%1...

C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	25600
Entropy (8bit):	5.584698658834256
Encrypted:	false
SSDEEP:	384:zKIhxI3PKZ/COyNcx5GTyoNr9MUVO9FvB3RH++x5XrIQP8S8cB5vWMiG:zKIhxI3PKZ/bIaqyCrXV+v1NrnLB5X
MD5:	7F7F391491C315A4A72EFCAC0D34FA93
SHA1:	20A18C7EA14F4E1D3044091B46D6E862B6F38708
SHA-256:	022577F47FB074B7D942C8F01DAAC778B110A373DE03B3B5043E887995B09D52

C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	
SHA-512:	78D39D7FD02D4F6CA0E13D0EACADC842D5A104C31342202875F84A69C310ECF6D4DCC8F00E95B09DE936922BE0312CF956C5E955254A99113EFB3F51E26C08E
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 2%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: document-37-1849.xls, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n.].*.3.*.3.*.3..)..+.3..)..).3..)..>.3..)..%.3.*.2.V.3..)..9.3..)..+.3. .)..+.3.Rich*.3.....PE..L...-.[R.....B...$.....J.....`....@.....k....@..... .....$q.....0.....h!..@..... .p..$.....text...|A.....B..... ..`.data.....`.....F.....@....idata..6....p.....H.....@..@.rsrc.....P.....@..@.reloc.....Z.....@. .B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Windows User, Last Saved By: Windows User, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Jun 2 14:40:34 2021, Last Saved Time/Date: Wed Jun 2 14:40:36 2021, Security: 1
Entropy (8bit):	7.59086745125602
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-47-2637.xls
File size:	92165
MD5:	92dcc47a1a044fc3a2328ec6eef3918b
SHA1:	6f9266a6c0b702cbaa0a3583df5c8cd1357eae35
SHA256:	ac4b99079b1ceb11db593097e421de9d9092765feedc23a3ab8ef912b292c988
SHA512:	fcd4b7c0a4e0f785604f40e0a9a4690e9b642223ee63088c6c4acfc262a18f5a79c77ab82498b422b229eaecc9a2e745b7e455c43ad2a85794e7adbac6b9bafd
SSDEEP:	1536:Lc2ZSmXWCQnp2c90Hg+j8z3kVfKIDVzoFGUsllB54N+wl8MYBzaVt4J5aukGqu:LXZxXTQ8hHgNQNeF3V4NvuhBzaV+J5a+
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-47-2637.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	

Indicators

Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1252
Author:	Windows User
Last Saved By:	Windows User
Create Time:	2021-06-02 13:40:34
Last Saved Time:	2021-06-02 13:40:36
Creating Application:	Microsoft Excel
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 23:34:00.419603109 CEST	192.168.2.22	8.8.8.8	0x78b6	Standard query (0)	webhub365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 23:34:00.490926981 CEST	8.8.8.8	192.168.2.22	0x78b6	No error (0)	webhub365.com		198.244.146.96	A (IP address)	IN (0x0001)

HTTPS Packets

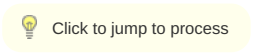
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 10, 2021 23:34:00.649437904 CEST	198.244.146.96	443	192.168.2.22	49165	CN=webhub365.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jun 08 19:53:43 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 06 19:53:43 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1204 Parent PID: 584

General

Start time:	23:33:34
Start date:	10/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fbd0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 2668 Parent PID: 1204

General

Start time:	23:33:39
Start date:	10/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c copy '%ProgramFiles(x86)%\Internet Explorer\Ext Export.exe' C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe
Imagebase:	0x4a9f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: nnAzot.exe PID: 2628 Parent PID: 1204

General

Start time:	23:33:41
Start date:	10/06/2021
Path:	C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe
Wow64 process (32bit):	true
Commandline:	'C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe' C:\aZ8ThU0Y\ERdZMUem GdPT AuMr7
Imagebase:	0xc80000
File size:	25600 bytes
MD5 hash:	7F7F391491C315A4A72EFCAC0D34FA93
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 2%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis