

ID: 432941
Sample Name: document-47-2637.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 00:00:08
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report document-47-2637.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 10
Static File Info 14
General 14
File Icon 14
Static OLE Info 14
General 14
OLE File "document-47-2637.xls" 14
Indicators 14
Summary 15
Document Summary 15
Streams 15
Macro 4.0 Code 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTPS Packets 15
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: EXCEL.EXE PID: 1204 Parent PID: 584 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Moved 17
File Written 17
File Read 17
Registry Activities 17
Key Created 17
Key Value Created 17
Analysis Process: cmd.exe PID: 2536 Parent PID: 1204 17
General 17
File Activities 17

Copyright Joe Security LLC 2021

File Created 17
File Written 17
File Read 17
Analysis Process: nnAzot.exe PID: 2380 Parent PID: 1204 17
General 17
Disassembly 18
Code Analysis 18

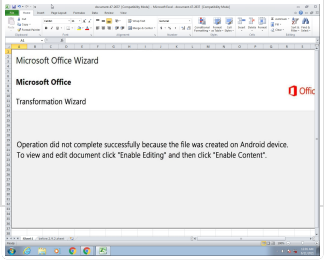
Analysis Report document-47-2637.xls

Overview

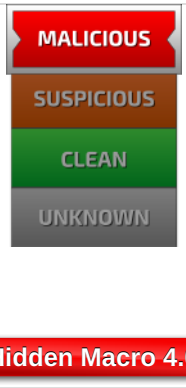
General Information

Sample Name:	document-47-2637.xls
Analysis ID:	432941
MD5:	92dcc47a1a044fc..
SHA1:	6f9266a6c0b702c..
SHA256:	ac4b99079b1ceb..
Infos:	

Most interesting Screenshot:



Detection



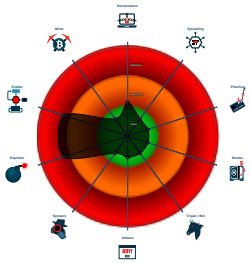
Hidden Macro 4.0

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: 2536 cmdline: 'C:\Windows\System32\cmd.exe' /c copy '%ProgramFiles(x86)%\Internet Explorer\ExtExport.exe' C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
  - nnAzot.exe (PID: 2380 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

Copyright Joe Security LLC 2021

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)

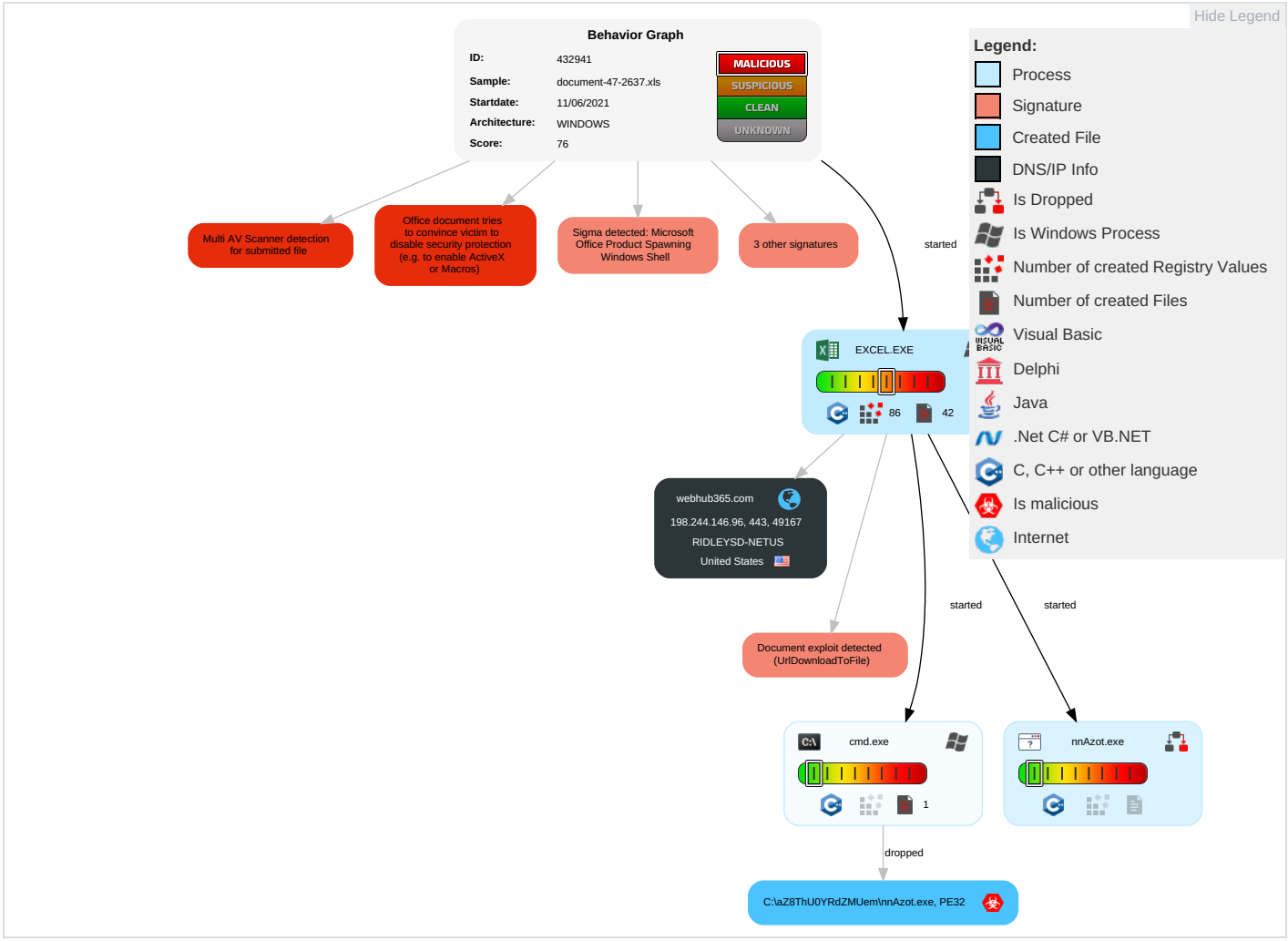
Found Excel 4.0 Macro with suspicious formulas

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	

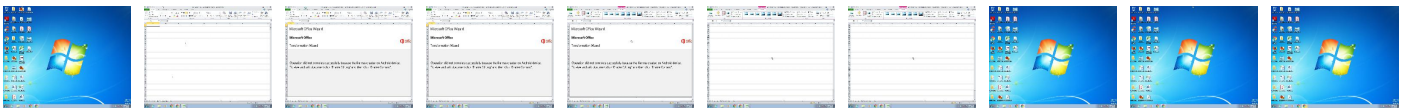
Behavior Graph

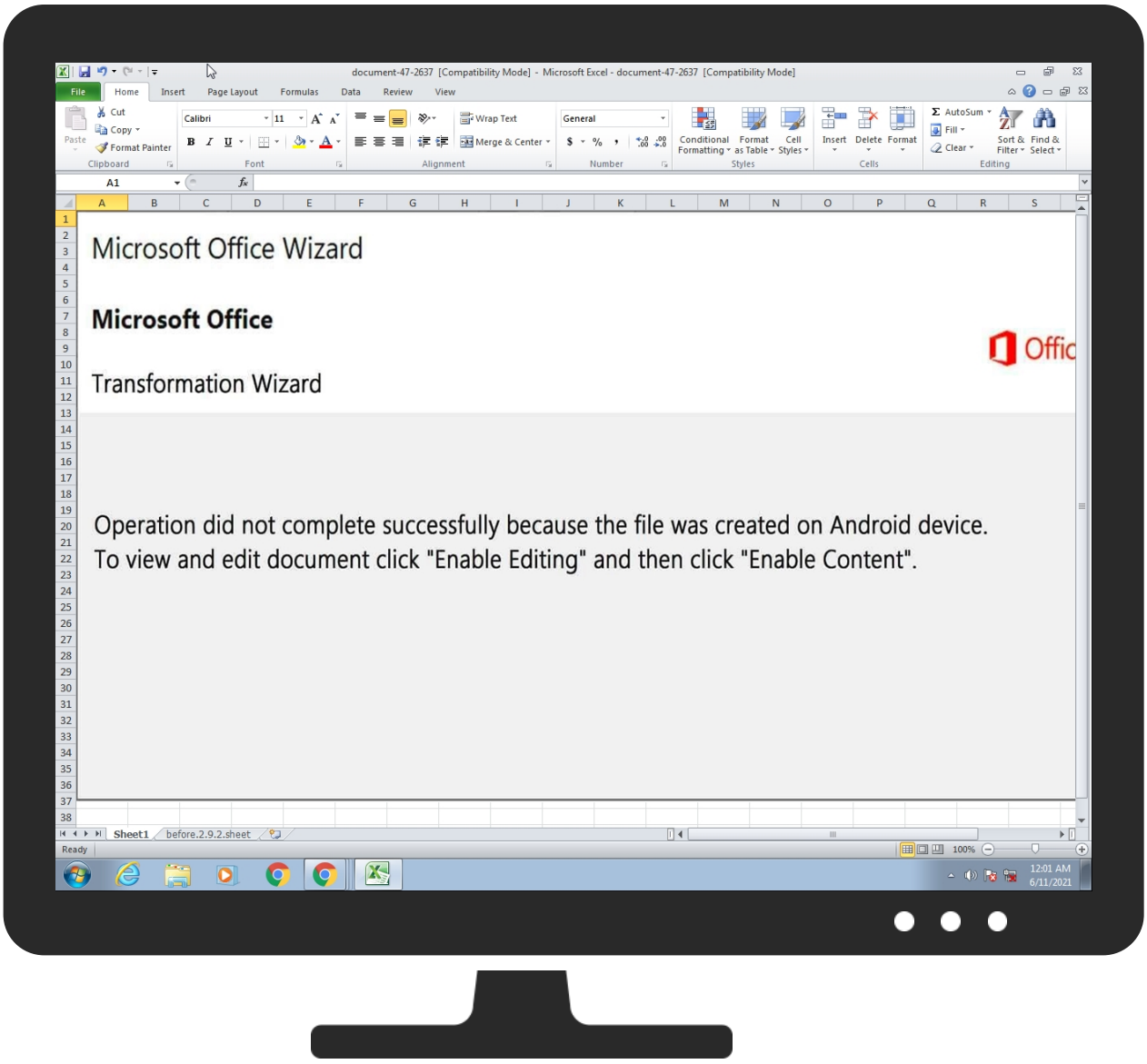


Screenshots

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

Copyright Joe Security LLC 2021

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:	432941
Start date:	11.06.2021
Start time:	00:00:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
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:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 88.6%) • Quality average: 72.3% • Quality standard deviation: 34.5%
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

Copyright Joe Security LLC 2021

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.244.146.96	document-47-2637.xls	Get hash	malicious	Browse	
	document-47-2637.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
webhub365.com	document-47-2637.xls	Get hash	malicious	Browse	• 198.244.146.96

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RIDLEYSD-NETUS	document-47-2637.xls	Get hash	malicious	Browse	• 198.244.146.96
	document-47-2637.xls	Get hash	malicious	Browse	• 198.244.146.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	document-47-2637.xls	Get hash	malicious	Browse	• 198.244.146.96
	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

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	document-47-2637.xls	Get hash	malicious	Browse	
	document-37-1849.xls	Get hash	malicious	Browse	

Copyright Joe Security LLC 2021

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
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wlEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ: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:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E154941554498 30D2809C8CF218D0B9196EC646BC
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*.?II..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):	3.1225789902305854
Encrypted:	false
SSDEEP:	6:kKLgNie8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:D78kPlE99SNxAhUe3OMx
MD5:	9332649BE2B7EEB84D2A51B4FCB8C610
SHA1:	EC5B37F58C8810F61A0978167001D6CAEE4CF14D
SHA-256:	B818B209B0885F643CECD70C1447B3D3C4547F7C7D2884195D19E2AFFC81A42D
SHA-512:	EB42861F3768F3B86281BBDB86702AA552E46F6CD4B38C215545ADFF820B905ED61B45B40C49B8B97EBF65462F796DA4EE5707F3B241CD24F9033858DA8AA2B
Malicious:	false
Reputation:	low
Preview:	p..... .....r~.^..(..... .....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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Entropy (8bit):	3.0169823334697616
Encrypted:	false
SSDEEP:	3:kkFkluAVfllXlE/JADkdllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yWJ/fdl/:kKWYADk5liBAIdQZV7QWB
MD5:	5604964BDBEBD78FC30DCCFE0D288FBC
SHA1:	CFB823EC2DC190DB7B1B6273EA727DBE29968A9D
SHA-256:	B7C960629B8D092922FC3F8FAEEC71203CA8F0576026D3167745439AA3108D72
SHA-512:	1499517A5F36BBFE8FE8D4460FCD94564DD6DD53610207A9B715F81BDC504CE306E65246668BABAEC6C3694D300CFBBB4DFAEE48E21E43EE8194083EE2A0F5E8
Malicious:	false
Reputation:	low
Preview:	p..... ....`... G0~.^..(..... .....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\CabE004.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.:..vI..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\F6DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	68561
Entropy (8bit):	7.608770850697448
Encrypted:	false
SSDEEP:	1536:m+yXkNLPHqvAk/Vi6+YDT7Hbc8hxCCV25Z:m+yUNLP4lA6+YHcId25Z
MD5:	B67C936515D2A419269AB8E2D93204DE
SHA1:	44331DB15B55BAD0D97DEFE091ACF39EE39248A3
SHA-256:	E933C429EFC848987756125BFE9C3AB422F5E2EFCAEF5F945718AC31F90C9658
SHA-512:	6B3D48B0153F8AC2D2AC7A4FB9462E145321D13AFD8C9284A94837DC5108FD55998CA902B7FD8EC83A8549F5A0B3B8CA4C7B951818AE04B03CF578BC3F5DA20
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\TarE005.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

C:\Users\user\AppData\Local\Temp\TarE005.tmp	
SHA-256:	07FDF8BC502E6BB4CF6AE214694F45C54A53228FC2002B2F17C9A2EF64EB76F6
SHA-512:	8AFC5D0D046E8B410EC1D29E2E16FB00CD92F8822D678AA0EE2A57098E05F2A0E165858347F035AE593B62BF195802CB6F9A5F92670041E1828669987CEEC7DE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..d...*.H.....d.0..d....1.0...`.H.e.....0..T...+.....7.....T.0..T.0...+.....7.....L.E*u...210519191503Z0...+.....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 06:00:40 2021, atime=Fri Jun 11 06:00:40 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.480521840960962
Encrypted:	false
SSDEEP:	12:85Q8LoLgXg/XAlCPCHaXtB8XzB/04uX+Wnicvb63+bDtZ3YilMMEpxRljKtTdJP8:85I/XTd6jJuYe4SDv3qArNru/
MD5:	D1901B672D68B95B87925635D8835BDF
SHA1:	3B0CAF79347B90E7F276CB084D1074E24599E8A2
SHA-256:	DB6552B4D3F6608CE90336C480BEC6C4E963B8815E377D16E895B186F040AA34
SHA-512:	83D9FFBF227CCBF7539E2DBFD061F446FD7107CDB06FF3967499214442C0EF4E1B23E50B481E85991ECFE0E794C73A8A4CF6DD71359C7B75BAEF747455BA033
Malicious:	false
Reputation:	low
Preview:	L.....F.....7G...z=}.^...z=}.^.. .....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.....R.8..Desktop.d.....QK.X.R.8*..._=.....:.....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\..#.....\\067773\Users.user\Desktop.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L 8C....&.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.....067773.....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 14:08:14 2020, mtime=Fri Jun 11 06:00:40 2021, atime=Fri Jun 11 06:00:40 2021, length=92672, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.536758685214297
Encrypted:	false
SSDEEP:	24:8i/XTd6jFyq4Me431Dv3qAdM7dD2i/XTd6jFyq4Me431Dv3qAdM7dV:8i/XT0jFB4MdEAQh2i/XT0jFB4MdEAQ/
MD5:	709594534DD8AAF9078F756A8817A71A
SHA1:	1FAF88E21AE6ED12EAE26EB687EEC62C97B6D7F2
SHA-256:	C411BE565BE4A1C8D52CB9FD1510C1CC565F34BCAE4385966579D84C325C74D1
SHA-512:	DF93EE96B3EC505691231141EBEF51DB12E8DB0CBC416584E27A8A4C4D9F31E181CC095F27FD21DB1CF709B0C8350CDB0867F3E9308DD3359890EF03010C8C 1
Malicious:	false
Preview:	L.....F.... ....}..{...z=}.^..E.G}.^...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.8 .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\..#..... ...\\067773\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.....067773.....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:	6C9C7CAFA742354DB174653D4C1CF9521AC10C67177FB2E26A85AE1267F1A45094BD1F1AE3C0B53836D5210F6083906F17C26A28A197D0CCF2F76D7447272E4
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\ZH9NG0C7.txt	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	99
Entropy (8bit):	4.738309873166655
Encrypted:	false
SSDEEP:	3:12mZI6A3xQlGTKvUQ2NwS2TdeX3Rsa/n:8YIr3xUGZXN2TwXzn
MD5:	1013A2F28CACF36A2234BC56C8B76B40
SHA1:	25B9130C97E0351F0707D53C72E4E1C700C324BE
SHA-256:	4B034D46F013E42559260BD248B7B0011EE83AE4D836D14FB4083A3BE287C3D2
SHA-512:	F28E38E260D8F9B5ADC14C6F449299D6318268412C2BDC9616E46CD9C22AF6DD5546F4684F549EF2FA8B1AD00400370AD2C84BD9ED4DC6704427B7D4EC7ADE3
Malicious:	false
IE Cache URL:	webhub365.com/
Preview:	PHPSESSID.hodlph97qarho6n2q5ae7qthj6.webhub365.com/.1536.1170067456.30891789.2127077170.30891663.*.

C:\Users\user\Desktop\774F0000	
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):	7.932017898229176
Encrypted:	false
SSDEEP:	3072:VKZ1QaE1iFKbbG46fQWnPdkuiZpKZ1SaE1/:VKZW9ocW46fjF8ZpKZ49l
MD5:	1C3608A1D6C608CAAB12624DE264B8DC
SHA1:	A83808D92C7633E5123DA9A49FA5F01F9836A256
SHA-256:	9ACD9A818075B4FA763A7B0328DB449DA693309C6EBE330B8C81F14BE566CD91
SHA-512:	4A407DA6AA2A6896391D8C967E18A516B01046D96E7A167A7EDBE4A0FBBCBC73407A72B82137452674142CDE33802B46E1081C0C5C769306736E8A9AAAADE46F
Malicious:	false
Preview:	.....g2...../.....X.:...5.IE..1`.3>...."n.^...}.6...Q.nKJD4.]..$.8.....g2...../.6.....X.:...5.IE..1`.3>...."n.^...}.6...Q.nKJD4.]..$.8.....*U....\.p.p.h`.q._.C.%5R."h.sHV-.. ..1.....K.. ..<...7].1..s.Ye....bsn.....!..g.<.....$N*'.~..apH.z*\..A{./.97ViB....7a.....=.....y.....@.....a=....i..,....TC.....R@....'....7"...z.....1.....d._..u.Db .R..h...o.1a9i.k..1...u.....@..O...B...$..3....1...).@q../Y.1...,.....u..1.....7.D.]...{...-.IGFB...e....1....L...C.D...:.i..$..f.:..U..1.*.P.'8 ..S.mX.S..XU...<'\e...Kl.>.j.q.p.0.1.....R ._<@..s}..aw l.....1...l....S.[B...).....1 w.W.`.1.1.....r."aiE?D.Z..0i.}...V..C5.-.1.....c.=>J.z.....:.m.}.arH..!.1...[.....aB.F|S.....;."....W;b.1....=x.....T.K...3,.PP..H..s..Y-1...i.%.....w..o}.-....-..lj..5..1.....F3.. 4.....;...2;...x.s^.1...o.....@.I.icN.{..M.".!b...1....P.r.r.'.G.H.....n...h...(6.1....=..V.2.....4.....iy..:F.1...

C:\Users\user\Desktop\C7DE0000	
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):	7.9268262065554325
Encrypted:	false
SSDEEP:	3072:M2hpEu0A4iQEmRqwJOu3J5Pn/cOGWJPn/cZGW02hpEA0w:V0tA4idvu3JRFBoN0/w
MD5:	388CD90E27FA7C09A02E5490E32F9408
SHA1:	0E61310B0D55D8C1E24DCBBC9CAA79874959E308
SHA-256:	EDA8CD37F5999158DCABBD39B4292FE7692163FBCEEB68AE1BDE1166D350564B
SHA-512:	6DA5A552A3ED2229C478AAE92AAAF5436B8F6D9C2DABFD580389DA3243B486C4B7EED5748C753D57123EF474455A77EA64373AC94EE2AEE24B5D872A6268BFAC
Malicious:	false
Preview:	.....g2...../....._`.....G4.'.3P_....P...@.....*]L..V.1.....g2...../.6....._`.....G4.'.3P_....P...@.....*]L..V.1.....T....\.p.S.T..~.|.`..C.0.J....hN~..\x9:..;i..~.{.I k.1...Z.\Q.....!JG..HB....}.Mu.....i.>It.W.....T.....[A.B....xa....!....=...e\.....^%.....:.....2m=.....Y..) .\.q.V...j.@....>....."...*.....v3....ly.....1...2....%i...J..F.:y.z.. ..B...X.1.....Bzme....Db.mD..i.....D..1.....Wi^..r..B.....h..Bp1...]*...gF.>. .....:9.I:U...\.1....u...c.....L.....-.....b1.*.._|..|..o....7..`y....e_.*:*..i..<o.>|1...S....~....7".5A&.I.$..p..v...1.. ...A0.....>.Vs.....3.z2...9.L1.....q.Q...=...Bz....N.$..g.Wl.1.....Km.9.....f..n.Q..}.&?)61.....E_..8E.-..4m).A)..H....O%1.....r...zA.s.....Nd..}.mj....q1...<.R.*..{.#...%....\Cc...?....1 ...e....C..O_....M.Ybz..>.SIX51.....n[....$...!....z\{D>?Hx...1.....ow.;xg'M.....y].L.|..3.1...Mp.BX."K.p.c.?.ojj..T.v|}?f..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

C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	
SHA1:	20A18C7EA14F4E1D3044091B46D6E862B6F38708
SHA-256:	022577F47FB074B7D942C8F01DAAC778B110A373DE03B3B5043E887995B09D52
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-47-2637.xls, Detection: malicious, Browse • 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+j8z3kVfKIDVzoFGUsIIB54N+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

Indicators

Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
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 11, 2021 00:01:02.692508936 CEST	192.168.2.22	8.8.8.8	0x6029	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 11, 2021 00:01:02.758696079 CEST	8.8.8.8	192.168.2.22	0x6029	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

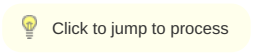
Copyright Joe Security LLC 2021

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 11, 2021 00:01:02.911695957 CEST	198.244.146.96	443	192.168.2.22	49167	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:	00:00:38
Start date:	11/06/2021
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:	0x13f660000
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

Copyright Joe Security LLC 2021

File Moved

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 2536 Parent PID: 1204

General

Start time:	00:00:43
Start date:	11/06/2021
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:	0x4a6e0000
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: 2380 Parent PID: 1204

General

Start time:	00:00:45
Start date:	11/06/2021
Path:	C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe
Wow64 process (32bit):	true
Commandline:	'C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe' C:\aZ8ThU0Y\ERdZMUem GdPT AuMr7
Imagebase:	0x3a0000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021