ID: 438634
Sample Name: idea-22543577.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:08:44
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

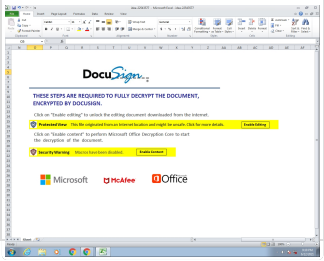
Windows Analysis Report idea-22543577.xlsm

Overview

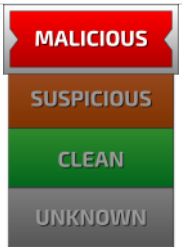
General Information

Sample Name:	idea-22543577.xlsm
Analysis ID:	438634
MD5:	690a255b0f1b59b.
SHA1:	1036eaadc0201b..
SHA256:	2aba85eff52ce4b..
Infos:	

Most interesting Screenshot:



Detection



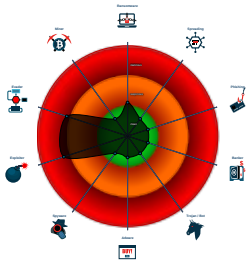
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Excel documents contains an embe…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- May sleep (evasive loops) to hinder …
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2492 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2352 cmdline: regsvr32 ..\wail1.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2392 cmdline: regsvr32 ..\wail2.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **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

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

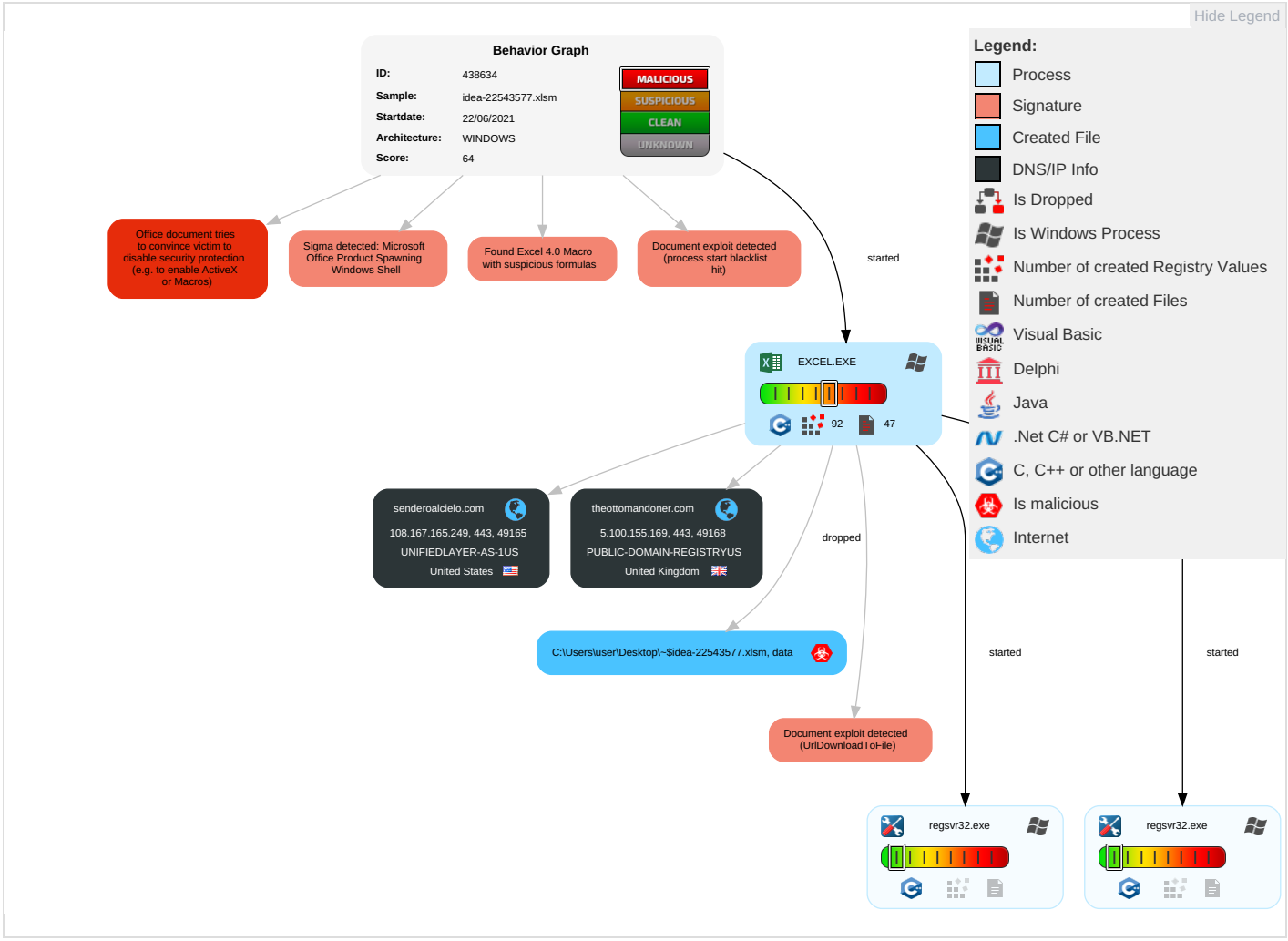
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1	Regsvr32 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatior
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

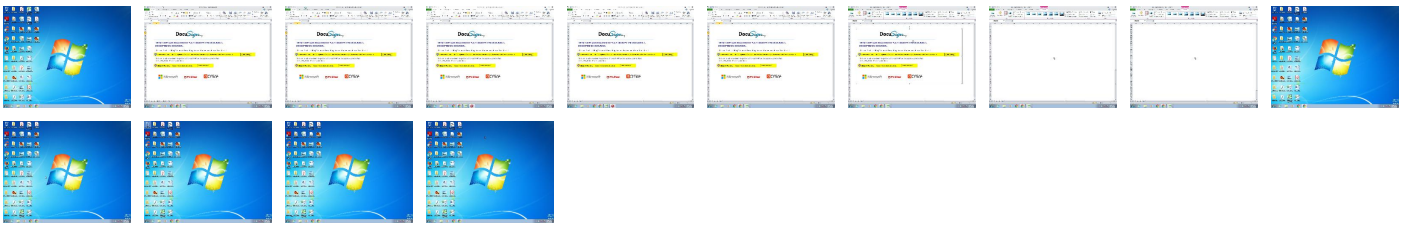
Behavior Graph

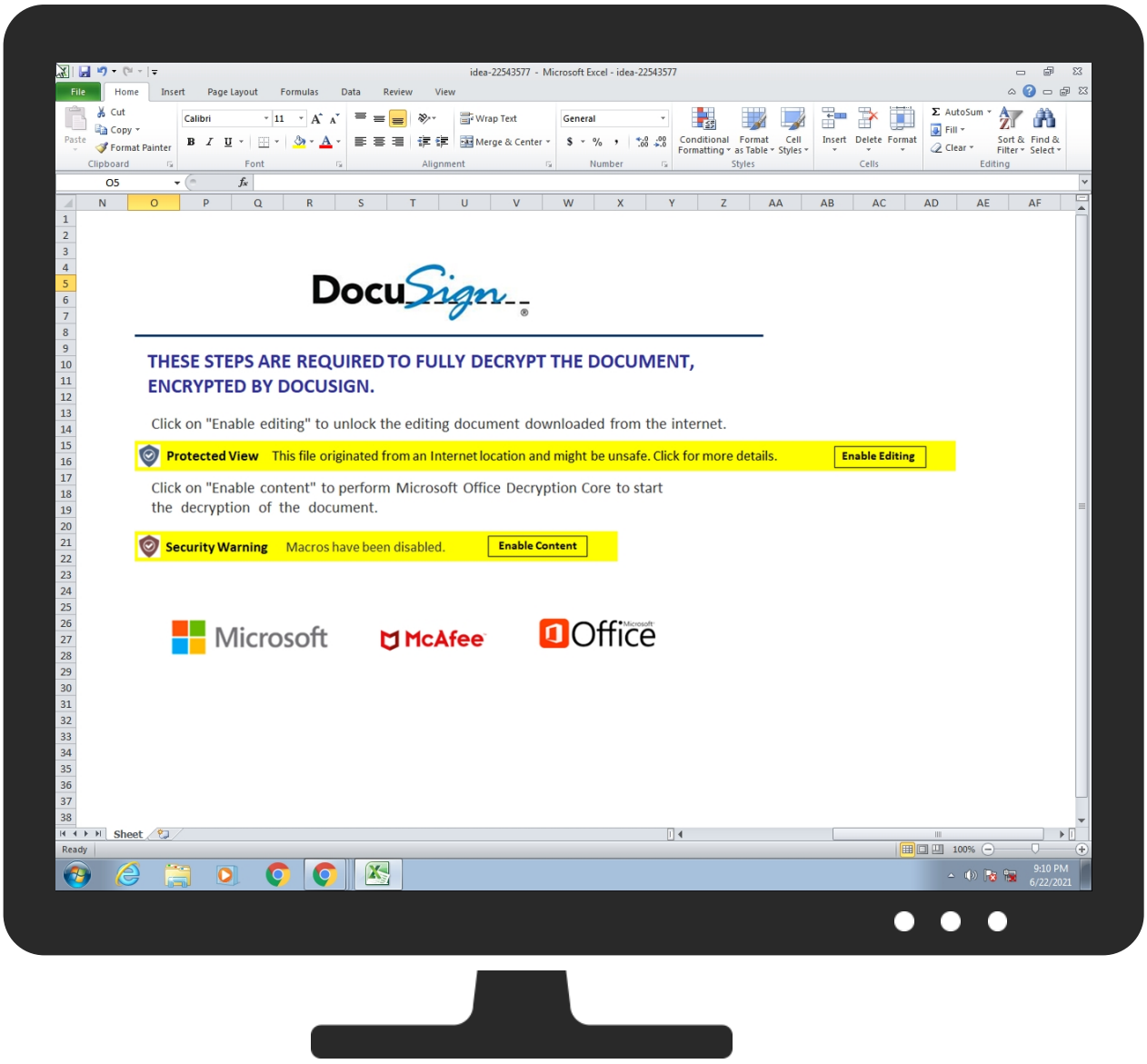


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theottomandoner.com	5.100.155.169	true	false		unknown
senderoalcielo.com	108.167.165.249	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.100.155.169	theottomandoner.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
108.167.165.249	senderoalcielo.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438634
Start date:	22.06.2021
Start time:	21:08:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	idea-22543577.xlsm
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:	mal64.expl.evad.winXLSM@5/13@2/2
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 • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:10:01	API Interceptor	2x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.100.155.169	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f62616e636f2e7074	Get hash	malicious	Browse	• y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f626116e636f2e7074

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Fra8994.exe	Get hash	malicious	Browse	• 162.241.60.126
	WXs8v9QuE7.exe	Get hash	malicious	Browse	• 50.87.146.99
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	Order.exe	Get hash	malicious	Browse	• 108.167.183.94
	Habib_Bank Payment Advice.doc__.rtf	Get hash	malicious	Browse	• 162.144.79.7
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 74.220.199.8
	FidKy67SWO.exe	Get hash	malicious	Browse	• 192.254.185.252
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 50.87.249.240
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 192.185.21.116
	idea-1232922316.xlsb	Get hash	malicious	Browse	• 162.241.194.107
	Orden de compra.exe	Get hash	malicious	Browse	• 192.185.0.218
	Drawing.exe	Get hash	malicious	Browse	• 162.241.61.229
	aim-1028486377.xlsb	Get hash	malicious	Browse	• 192.232.222.161
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 162.214.148.174
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.61.218
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 74.220.199.8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Lebanon Khayat Trading Company.exe	Get hash	malicious	Browse	• 192.254.185.244
PUBLIC-DOMAIN-REGISTRYUS	Fra8995.exe	Get hash	malicious	Browse	• 208.91.198.143
	Fra8996.exe	Get hash	malicious	Browse	• 208.91.198.143
	Fra8997.exe	Get hash	malicious	Browse	• 208.91.199.223
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 103.50.160.62
	aim-1028486377.xlsb	Get hash	malicious	Browse	• 103.21.59.25
	7qVSiXSTdETO7cX.exe	Get hash	malicious	Browse	• 208.91.198.143
	PI Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment Advice Note from 21.06.2021 to 608720.exe	Get hash	malicious	Browse	• 208.91.199.225
	Inquiry pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	HYr6YeH1RP.exe	Get hash	malicious	Browse	• 208.91.198.143
	fng1AXSgue.exe	Get hash	malicious	Browse	• 208.91.199.225
	memorandum.exe	Get hash	malicious	Browse	• 208.91.199.223
	Bank Betails.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.854.8381.exe	Get hash	malicious	Browse	• 208.91.199.233
	AWB & Shipping Documents.exe	Get hash	malicious	Browse	• 208.91.199.224
	order no ORD00404083_01.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#4500484210.exe	Get hash	malicious	Browse	• 208.91.199.233
	Request for Catalog and quotation.exe	Get hash	malicious	Browse	• 208.91.198.143
	INQUIRY pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	Img-347654566091234.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	tender-1235416393.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	TT_COPY.MT103.SWIFT.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	MT103.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	Purchase_Order.doc	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.19092.rtf	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	aim-1860610262.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	otKl5DLaUo.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	idea-1127603629.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	idea-1134058065.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	idea-1132671574.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	idea-1128721882.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	idea-108527315.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	idea-112755060.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	viru.xls	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	viru.xls	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249

Dropped Files

No context

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, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{..,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.[]}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.139205445116624
Encrypted:	false
SSDEEP:	6:kKnqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:/G5kPlE99SNxAhUe0et
MD5:	64F47B9C43BAE5277D277962EBE6B766
SHA1:	5FC06F8F587C2B0990F7B86A81468D4553E1941E
SHA-256:	E101892B3DC24393E9D0DE69BA0BE4F15F148FE885DA47FC14D89137821DD338
SHA-512:	A5E5D85077EE4466844493A8464E50D91D549C78E2BBCF3DC9E15679A048A8532A82750326BAB0AF5846026DA93D992ADE5693957C32C22CAA8BBC7291DE6A4
Malicious:	false
Reputation:	low
Preview:	p..... ....\.I..g..(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.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):	2.978677724097254
Encrypted:	false
SSDEEP:	3:kkFklUPCFltfllXIE/2S+HDHllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yR5B:kKPP6q+HDXliBAIdQZV7QvB
MD5:	BD01DD8813FECD8323BA8C64391FDDBD
SHA1:	63B8A0DB9C7621EE03A77EA0922C924A081DD293
SHA-256:	E1E0D1415E227658E1D5D35FAD6D9E6398335D90C30916168D45DA2814B40705
SHA-512:	F22BAEF01A731A9F90B70A8AA76D5C22961B913D29A1A31BD798028051B0D560679D0057E5EF1D5EEADF5F8383D3D2E6657F813D2AA7098417C8A6AEA0027BC
Malicious:	false
Reputation:	low
Preview:	p..... ....`...t....g..(..... .....S`..b.....(.....}...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.4.d.2.e.5.9.c.f.b.8.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DA3B3626.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1133 x 589, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	75711
Entropy (8bit):	7.915372969602997
Encrypted:	false
SSDEEP:	1536:gxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncT:7br0o45GUgHhX8jC9yST
MD5:	8296338A43942E3107802E3062AC1270
SHA1:	46E67A586ED8A961AF7FD03140547C1CB2BAC227
SHA-256:	BE5F61F2AE8E4C9F9ADBCE5EC33D4C01A331734FFC5818AA8E45CF60456C5ABD
SHA-512:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171AD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...m...M.....p.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....g.....q.|.....<...'r....-^..c.If.,ffX1K.[....Z....V.LO5L..J+...z.]]u..>.==.....Q.....(.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....j.7ZP...:...0S....z5T.....).WU=j.*.$H.B.P.)I.6Q..'.I..7..k..J.o..._....6..{C...r.\|2W.[a...m.BI.?...5.....D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._.,..I.\|a.7+>.....A#.....3v..37.....w(..j..C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..\|..d../.....vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.....#!...T...C.#.>.E,[.,.....E....h~B.Y./....(2.....(...`....~w#.%..R..{.....N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q..."...W2.....Q...G...z....Ea.....

C:\Users\user\AppData\Local\Temp\A8FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	93170
Entropy (8bit):	7.834723143895331
Encrypted:	false
SSDEEP:	1536:o+xJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5nchya2/WV1AWae:o5br0o45GUgHhX8jC9ySosV1AWae
MD5:	8B497571E546A76BA893845F6A02FBE6
SHA1:	39CB9CB427D51BFD0FD00583697C7DB2EABD5DE0
SHA-256:	90609936B034B48E247760523F47BC87F9E2977E687B5F16CA67FFA8ED16A57A

C:\Users\user\AppData\Local\Temp\A8FE0000	
SHA-512:	A3756B37F91E4220281D3711A95FBB433439F5CF42751E652DAC8D9FDEF9A862512088AB93FB1001085870C1F2D824D6BDCD29DE75597BFD2145AFFCFD3B28D
Malicious:	false
Reputation:	low
Preview:	.Mn.0....z...B...AQX.M.m.....D.".....V..p,.q...y..#...r....jgkvVMX.V:.mS..?./..(...Y....]....=`A..k...r...N`.<X.Y..H...^.h..O&.\:...2&.6.~...3..Z..M&smY.m.^B.Lxo.....V.@J.Xh.....+..... v..A.1.@.T.2...m...].9=.....N.@....E.R...?.Y/....>.q.h..VP\.....+..\X.[V.E.....`..X.....s.4&.}...)G".....K.d.#.8.Oyd.zCh..l.!E=.....".-nL.'.}.a..q.....mq....i.....H.....6.#.9f?...[.@.D....'.\{ ...CJ.....:.Fx..G...w..M.....a....-.:.....O@.....c.....PK.....!.!=J.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Cab2A1.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2F A0
Malicious:	false
Reputation:	low
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{.,,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\Local\Temp\Tar2A2.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	158974
Entropy (8bit):	6.311775051607851
Encrypted:	false
SSDEEP:	1536:ilqXley2pR737/99UF210gNucQodv+1//dMrYJntYyjCQx7s2t6OGP:iQXipR7O/gNuc/v+lXjCQ7sO0
MD5:	E4731F8A3E7352DBA44EC7D3DD15BAEA
SHA1:	D5CA0025FBD356DEB8EDE35001F93039625562A5
SHA-256:	6C78EF77ACEF978321CCD30EE126FB7D30285BC186DDBDBE8B3E8F6E69D01353
SHA-512:	E68BA11A73E28404A274F0EE4ECC97A8BEFEDB91A20BDC5B00C72AE8928DD63924E351BE8A88E40960D54CE07E21EA21710DB0DFA00A5558C4264490E27B6988
Malicious:	false
Preview:	0..I...*.H.....I.0..I....1.0...`.H.e.....0..\...+.....7.....\.0..\.0...+.....7.....\.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=Wed Jun 23 03:09:49 2021, atime=Wed Jun 23 03:09:49 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.480231631115749
Encrypted:	false
SSDEEP:	12:85QxYLCLgXg/XAlCPCHaXgzB8IB/hhxkfX+WnicvbSubDtZ3YilMMEpxRljK1TdK:85jU/XTwz6IThuYepDv3qgrNru/
MD5:	380B060C6F20226A6B8100F1B331361E
SHA1:	ACA823307DC3D68CC49FB01AE11007AAF04AECAA
SHA-256:	E99E64441AA1B276E00F69BD1EC276B050255D6BD643D256B900A2F5A3E473CC
SHA-512:	BBD1DAE8FF75E159108867FA44CD0DD9225E4584DF95B43F7DA7AD561EDA50EFBC8D423CC4A6EA5CB98CAC1CD2713818E7EE538426B824C31A0C20AB4F3B0 1F6
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Preview:	L.....F.....7G.....g.....g...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.....R9!..Desktop.d.....QK.X.R9!*..._=.....:.....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\..#.....\\841618\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.....841618.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\idea-22543577.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=Wed Jun 23 03:09:49 2021, atime=Wed Jun 23 03:09:49 2021, length=93170, window=hide
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	4.548028650368087
Encrypted:	false
SSDEEP:	48:8B/XT3lkD+qngYenKgQh2B/XT3lkD+qngYenKgQ/:8B/XLlkD+aQKgQh2B/XLlkD+aQKgQ/
MD5:	BDA1647BFDEA0D79EC3F0B1A959CECE5
SHA1:	0D757F2C6F2C1673E45DA8C326A7FE6800DCADDA
SHA-256:	3CDD8EC7A1B662611CF4A3FE49A53CB5FBF5C67E4191E99C44A334493125B2BD
SHA-512:	4B46EA26B9553201842A2CEE6C50B754B9E850A070D82C885A73F8EF994F5B2CCD8F586EB5B0288266F701DE8B78FBD928CEDCD082A1C9711DF5B2081F61FF8D
Malicious:	false
Preview:	L.....F.... ....i..{..T...g.....g...k.....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.....n.2..l...R5! .IDEA-2~1.XLS..R.....Q.y.Q.y*...8.....i.d.e.a.-.2.2.5.4.3.5.7.7...x.l.s.m.....|.....-...8...[.....?J.....C:\Users\..#.....\\841618\Users.user\Desktop\idea-22543577.xlsm.).....\....\....\....\....\.D.e.s.k.t.o.p.\.i.d.e.a.-.2.2.5.4.3.5.7.7...x.l.s.m.....:..,.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.....841618.....D_....3N...W...9F.C.....[D_

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):	94
Entropy (8bit):	4.621739484560059
Encrypted:	false
SSDEEP:	3:oyBVomxWHzXdUlUBhXXdUlmxWHzXdUlv:dj07bxy7E
MD5:	E7873154CD23EE19AAA8800DC776A9B5
SHA1:	BB75A07FBBC9BE7C5F38BB058ED8198336C4F73C
SHA-256:	6E67DB062BE87713F064EF905334EB421CC07ABB115DD7975323EF1EDBAD4F13
SHA-512:	8844B76DFF4AF8A235E5B791ADD65A951FEF222C64450AC98D2F3C94F7B08791A1DC64F5DFECC90EE228EF82BB0D0918E6AE77E9E836D8541FD0F4934026D45C
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..idea-22543577.LNK=0..idea-22543577.LNK=0..[misc]..idea-22543577.LNK=0..

C:\Users\user\Desktop\69FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	93170
Entropy (8bit):	7.834723143895331
Encrypted:	false
SSDEEP:	1536:o+xJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5nchya2/WV1AWae:o5br0o45GUgHhX8jC9ySosV1AWae
MD5:	8B497571E546A76BA893845F6A02FBE6
SHA1:	39CB9CB427D51BFD0FD00583697C7DB2EABD5DE0
SHA-256:	90609936B034B48E247760523F47BC87F9E2977E687B5F16CA67FFA8ED16A57A
SHA-512:	A3756B37F91E4220281D3711A95FBB433439F5CF42751E652DAC8D9FDEF9A862512088AB93FB1001085870C1F2D824D6BDCD29DE75597BFD2145AFFCFD3B28D
Malicious:	false
Preview:	.Mn.0....z...B...AQX.M.m.....D."....V..p,.q...y..#...r....jgkvVMX.V:.mS..?./..(...Y....]....=`A..k...r...N`.<X.Y..H...^.h..O&.\:...2&.6.~...3..Z..M&smY.m.^B.Lxo.....V.@J.Xh.....+.....v..A.1.@.T.2...m...].9=.....N.@....E.R...?.Y/....>.q.h..VP\.....+..\X.[V.E.....`..X.....s.4&.}...)G".....K.d.#.8.Oyd.zCh..l.!E=.....".-nL.'.}.a..q.....mq....i.....H.....6.#.9f?...[.@.D....'.\{...CJ.....:.Fx..G...w..M.....a....-.:.....O@.....c.....PK.....!.!=J.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$idea-22543577.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$idea-22543577.xlsm	
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.835191332560826
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	idea-22543577.xlsm
File size:	93205
MD5:	690a255b0f1b59b3421800bab8b41c10
SHA1:	1036eaadc0201b50d3d005ad05e208888021b945
SHA256:	2aba85eff52ce4b7d41b651baec98fea810a3307dc2b90bebf1c68131018cb0f
SHA512:	a124c5e4e8cdacc52e84ab89e92f83cbf535b3757271fde02bdb8b9b254c10f1bc2a05e09ed2dc9f3b1f605f698da6970048ea4fc187375c860b745cb551f8d1
SSDEEP:	1536:CaxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncEya2/dLBT0y:Clbr0o45GUgHhX8jC9ySXDLB/
File Content Preview:	PK.....!.!=J.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "idea-22543577.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:	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 22, 2021 21:09:47.215919971 CEST	192.168.2.22	8.8.8.8	0xed69	Standard query (0)	senderoalcielo.com	A (IP address)	IN (0x0001)
Jun 22, 2021 21:09:49.944199085 CEST	192.168.2.22	8.8.8.8	0x4b51	Standard query (0)	theottomandoner.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 21:09:47.278036118 CEST	8.8.8.8	192.168.2.22	0xed69	No error (0)	senderoalcielo.com		108.167.165.249	A (IP address)	IN (0x0001)
Jun 22, 2021 21:09:50.025887966 CEST	8.8.8.8	192.168.2.22	0x4b51	No error (0)	theottomandoner.com		5.100.155.169	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
Jun 22, 2021 21:09:47.646414042 CEST	108.167.165.249	443	192.168.2.22	49165	CN=senderoalcielo.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.	Sun May 30 04:16:52 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 28 04:16:52 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 21:09:50.159957886 CEST	5.100.155.169	443	192.168.2.22	49168	CN=www.theottomandoner.theottomandoner.co.uk 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.	Mon Jun 21 15:18:17 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Sep 19 15:18:16 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

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2492 Parent PID: 584

General

Start time:	21:09:45
Start date:	22/06/2021
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:	0x13f710000
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: regsvr32.exe PID: 2352 Parent PID: 2492

General

Start time:	21:09:53
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\wail1.dll
Imagebase:	0xff4b0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: regsvr32.exe PID: 2392 Parent PID: 2492

General

Start time:	21:09:54
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\wail2.dll
Imagebase:	0xff4b0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Disassembly

Code Analysis