ID: 438318
Sample Name: plan-1637276620.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 13:26:27
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

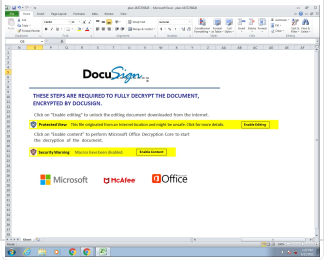
Windows Analysis Report plan-1637276620.xlsm

Overview

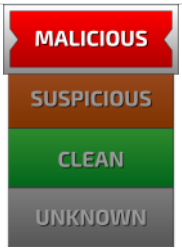
General Information

Sample Name:	plan-1637276620.xlsm
Analysis ID:	438318
MD5:	4d44784f088b8dd.
SHA1:	7d01c190b2e73c..
SHA256:	c63e0b01a696a0..
Infos:	

Most interesting Screenshot:



Detection



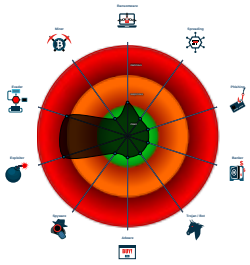
Hidden Macro 4.0

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: 2564 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2184 cmdline: regsvr32 ..\wail1.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 960 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:

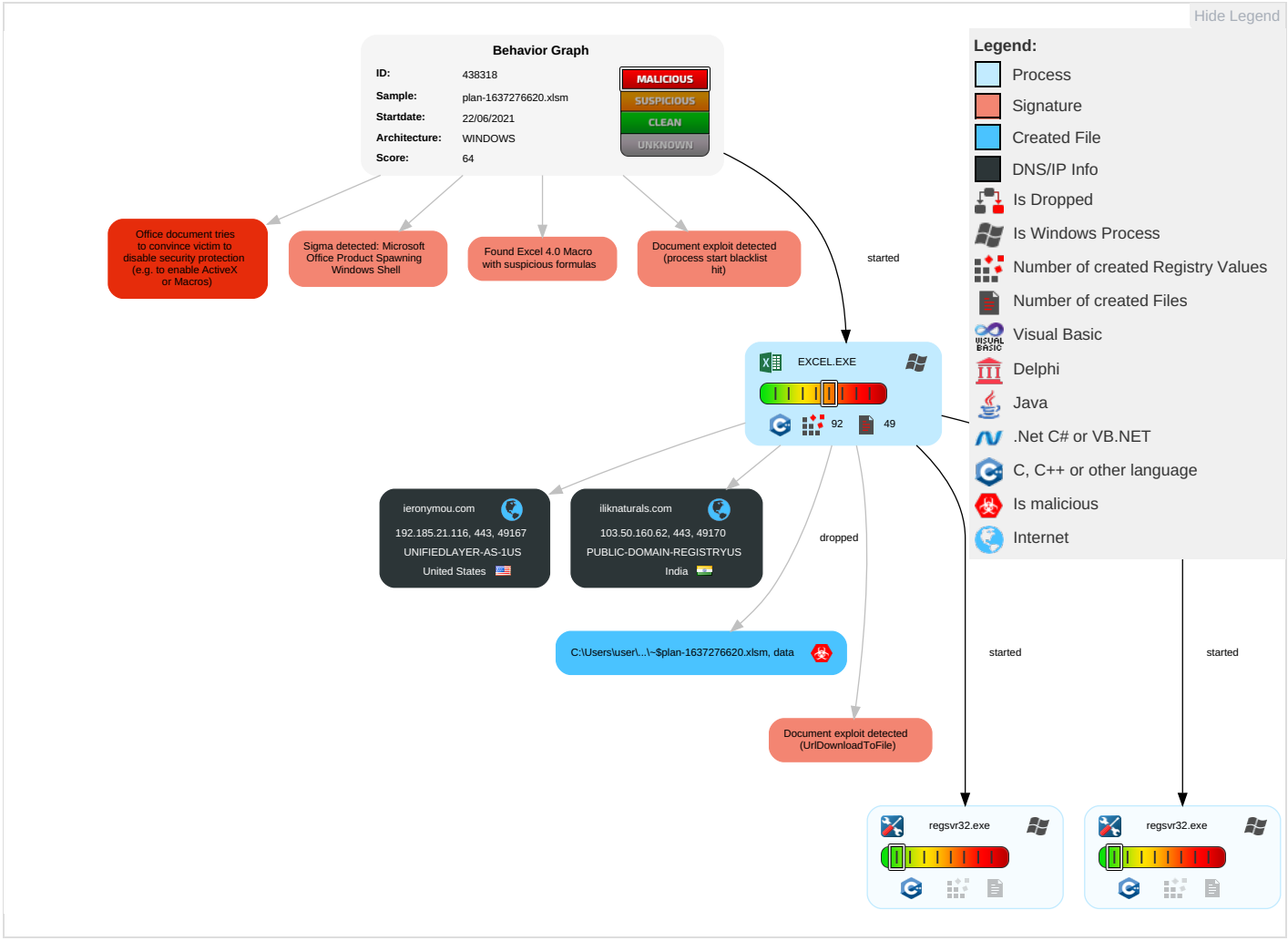
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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

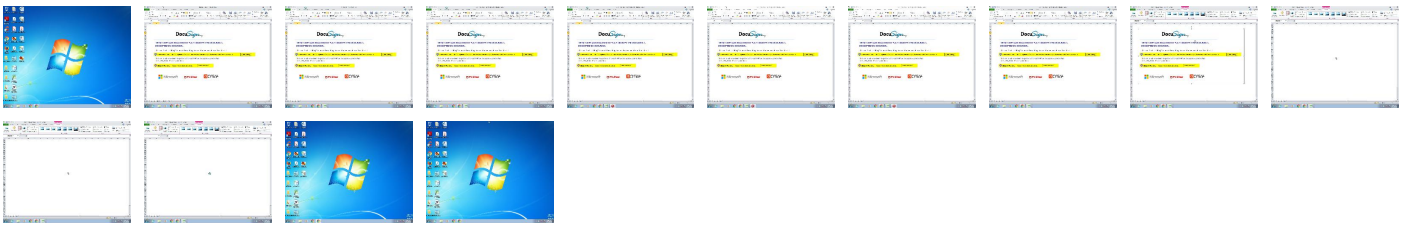
Behavior Graph

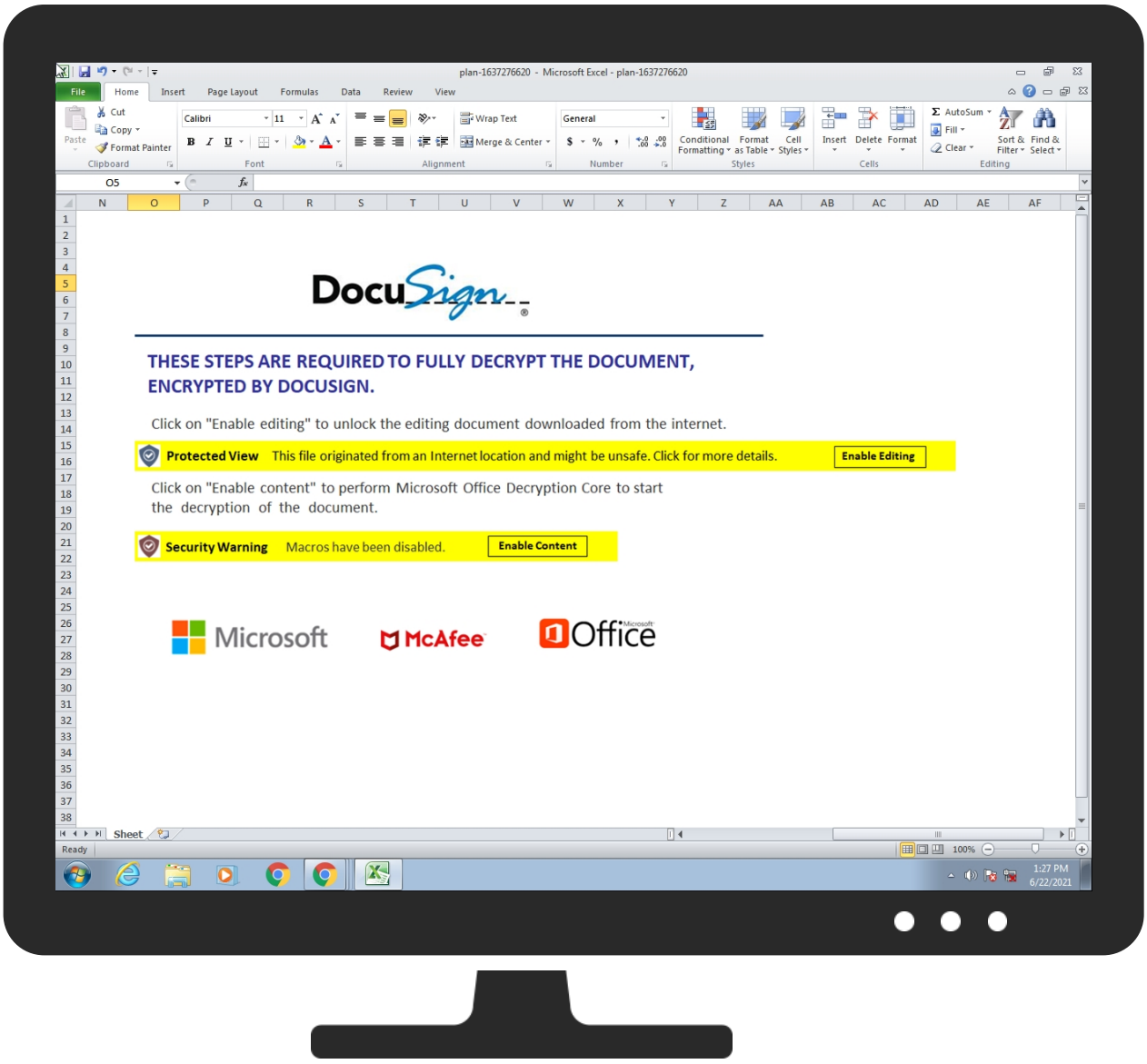


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
plan-1637276620.xlsm	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
iliknaturals.com	0%	Virustotal		Browse
ieronymou.com	3%	Virustotal		Browse

URLs

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

Source	Detection	Scanner	Label	Link
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	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
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://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
iliknaturals.com	103.50.160.62	true	false	• 0%, Virustotal, Browse	unknown
ieronymou.com	192.185.21.116	true	false	• 3%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.21.116	ieronymou.com	United States		46606	UNIFIEDLAYER-AS-1US	false
103.50.160.62	iliknaturals.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438318
Start date:	22.06.2021
Start time:	13:26:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-1637276620.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
13:26:54	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
192.185.21.116	Complaint_Letter_786544411_09072020.doc	Get hash	malicious	Browse	• hillsboro bookkeeping.com/yowyvoux/55555555.png
103.50.160.62	SecuriteInfo.com.Heur.2515.xls	Get hash	malicious	Browse	• www.pharmainstruelec.com/nezlzltik/590906.jpg
	SecuriteInfo.com.Heur.2515.xls	Get hash	malicious	Browse	• www.pharmainstruelec.com/nezlzltik/590906.jpg
	1921448169-12072020.xls	Get hash	malicious	Browse	• www.pharmainstruelec.com/nezlzltik/590906.jpg
	1921448169-12072020.xls	Get hash	malicious	Browse	• www.pharmainstruelec.com/nezlzltik/590906.jpg
	http://gabbargarage.com/lakw7z7/secure.myaccount.resourses.com/	Get hash	malicious	Browse	• gabbargarage.com/lakw7z7/secure.myaccount.resources.com/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	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
	Lebanon Khayat Trading Company.exe	Get hash	malicious	Browse	• 192.254.185.244
	Purchase_Order.exe	Get hash	malicious	Browse	• 50.87.249.240
	paw.exe	Get hash	malicious	Browse	• 192.185.20.31
	invoice.pdf.exe	Get hash	malicious	Browse	• 192.185.171.219
	eTWZtFRRMJ.exe	Get hash	malicious	Browse	• 74.220.199.6
	Purchase Order No. 7406595 .xlsx	Get hash	malicious	Browse	• 74.220.199.6
	Sampath Bank_Payment Advice swift.doc	Get hash	malicious	Browse	• 162.144.79.7
	purchase items.exe	Get hash	malicious	Browse	• 50.87.146.199
	aim-1860610262.xlsm	Get hash	malicious	Browse	• 192.185.71.128
	aim-1860610262.xlsm	Get hash	malicious	Browse	• 192.185.71.128
	Tcopy.exe	Get hash	malicious	Browse	• 50.87.146.99
PUBLIC-DOMAIN-REGISTRYUS	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
	Img-347654566091236.exe	Get hash	malicious	Browse	• 208.91.199.223
	KIkIc66LT4.exe	Get hash	malicious	Browse	• 208.91.199.223
	ORDER TSA-A090621B.exe	Get hash	malicious	Browse	• 208.91.199.223
	KaGC54QXnK.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	TT_COPY.MT103.SWIFT.docx	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	MT103.docx	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	Purchase_Order.doc	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.19092.rtf	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	aim-1860610262.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	otKl5DLaUo.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	idea-1127603629.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	idea-1134058065.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	idea-1132671574.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	idea-1128721882.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	idea-108527315.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	idea-112755060.xlsm	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	viru.xls	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	viru.xls	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	JPM Chase Remittance Advice.xlsx	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	cryptowall_dump.exe	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116
	Complaint details 1.doc	Get hash	malicious	Browse	• 103.50.160.62 • 192.185.21.116

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, 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\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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
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..:.pl.....:^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):	3.1263750649191113
Encrypted:	false
SSDEEP:	6:kKYse8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:As8kPlE99SNxAhUe3OMx
MD5:	53783EF032951E1DDF6C108E6D7C55BE
SHA1:	B9F2928787F636BCE4312A0DC2CB987F841DA0EC
SHA-256:	4D4EE6853F9C7BFA1D541D625ADBA1568306439929115163B2A4380BD05A7B33
SHA-512:	B79982962CDDE9FE0DB6267AA2222553E0E230C95D4E9D06EB0DE69C3F808897D78DD44AB311BD4ECDD92E20F88ED01DBEED2CDD79D779E54436633C3B99C A2
Malicious:	false
Reputation:	low
Preview:	p..... .....g..(..... .....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):	2.9959337381670825
Encrypted:	false
SSDEEP:	3:kkFklu6llltfllXlE/2S+HDHllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yR5B:kK2/q+HDXliBAldQZV7QvB
MD5:	45D2A58EE172CB6656E3D63AFDAFAC11
SHA1:	B23953FEE64157846B8155B65799BC81C69E50BF
SHA-256:	6DE4A4C23AFFB44601F5498917E3A91CF97095684F29F2EB7779BA52872FC314
SHA-512:	FAD79EE40B3E7ADA7C71265F615C850D8244B0F02B36D351ECD56D31A85BD8A896D3B2B849AFA51D9E23E645F1F442E3DB06DB437D463D4102B07B93702B4C 0
Malicious:	false
Reputation:	low
Preview:	p..... ....`.....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\F9EDFDD2.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:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171A D
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.*.$H.B.P.)l.6Q..'.l..7..k..J.o..._....6..{C...r.|2W.[a...m.BI.?...5.....D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._.,..I.|a.7+>.....A#.....3v..37.....w(..j.. .C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..|..d../.....vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.....#!...T...C.#.>.E,[,.....E....h~B.Y./....(2.....(..`....~w#.% ..R..{.....N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q..''...W2.....Q...G...z....Ea.....

C:\Users\user\AppData\Local\Temp\4ECE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Temp\4ECE0000	
File Type:	data
Category:	dropped
Size (bytes):	93153
Entropy (8bit):	7.835054103634326
Encrypted:	false
SSDEEP:	1536:oaxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncoclV1AWHP:olbr0o45GUgHhX8jC9ySogV1AWHP
MD5:	47C592EB97A153A45E1C51F969D8C787
SHA1:	9095E3626503E6B3F9FD173927A00FDDCB4B7234
SHA-256:	F779082667B29A95A2A60C3261C15C09BD80A414898FCFF2B1E7B528C940F8CD
SHA-512:	ED7A8E25541678B44242D5BCC5743F30CBAD3518E65E5DDE6A16FF61410450A1DD11B9A0365154B081F91CB539955C9C21191575CF365AD71E64D79A87C778E
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\CabDAC6.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\TarDAC7.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
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=Tue Jun 22 19:26:38 2021, atime=Tue Jun 22 19:26:38 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.491998857498724
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
SSDEEP:	12:85QxuNcLgXg/XAlCPCHaXgzB8IB/gUaX+WnicvbsaRbDtZ3YilMMEpxRljKkdMTg:851K/XTwz6IMYehtDv3qNArNru/
MD5:	64EB129663574FFAF3327CA9360299CB
SHA1:	5E4EBA6C1312336B58CA21CA178209371B69EA3B
SHA-256:	9963C2EA6DFD76705A3BA607DE78F7BE08042F9D8249EC0D6E8B9855FD5754EA
SHA-512:	A793C4BEF23E9A82DD772878AA07E83E245BA724056DDE6FD12A214BA444F4C7A8BF574EA50D45CD69835C0D2DC4EA973A3BE9A706E5027C9D298451B242FC6
Malicious:	false
Preview:	L.....F.....7G..S.a.g..S.a.g... .....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.....RT...Desktop.d.....QK.X.RT.*..._=.....:.....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\..#.....\\813848\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.....813848.....D_....3N...W...9r.[.*.....}EkD_....3N...W...9r.[.*.....}Ek....

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):	100
Entropy (8bit):	4.628814969776364
Encrypted:	false
SSDEEP:	3:oyBVomxWeqXWuNqXWumxWeqXWuv:djgGQqGaGg
MD5:	32693F1BBA06D4B8A5179CF03093DEAD
SHA1:	F575E24C8881BD57208B03CFA8361860C3AD5F7F
SHA-256:	BE869C5A0ECA3ADB50B587185C18633DBA657341B5B8022F57F49C33191189EA
SHA-512:	527A4FD652732FA8468344107AC5CB85BC0E93FBC24E7FA54505A7BD528779EAE57869CA7B540DA16CB41EA4BC7CDE5AE9DBE7E6031F45C30FCD7EC6EE669B2
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..plan-1637276620.LNK=0..plan-1637276620.LNK=0..[misc]..plan-1637276620.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\plan-1637276620.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 14:08:13 2020, mtime=Tue Jun 22 19:26:38 2021, atime=Tue Jun 22 19:26:38 2021, length=93153, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.512071638058982
Encrypted:	false
SSDEEP:	24:8gnS/XTwz6Iknoehz4Dv3qNAdM7dD2gnS/XTwz6Iknoehz4Dv3qNAdM7dV:8gS/XT3IkoGDNAQh2gS/XT3IkoGDNAQ/
MD5:	3E75EAB3A0105D7C163F0D643D69EDE8
SHA1:	158AE84392602D30FEB6E14AE350DA62EA84AD30
SHA-256:	A84C948DE21FB1B7682248E9433C7BEC4AE241476C0CA306A72DCFA20B92947F
SHA-512:	96F56751FA5667D4AE6489561DE8EF68E3A9AC5B5CACB631BB72D0D8ABEC58F433E725F36AF22CD4059D20F5B346A151E85B2E11F32A2DA25B4E1E58C70B2D0
Malicious:	false
Preview:	L.....F.... ...6.2..{....\.g..S.a.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.....r.2..l...RP. .PLAN-1~1.XLS..V.....Q.y.Q.y*...8.....p.l.a.n.-.1.6.3.7.2.7.6.6.2.0...x.l.s.m.....~.....-...8...[.....?J.....C:\Users\..#.....\\813848\Users.user\Desktop\plan-1637276620.xlsm.+.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.p.l.a.n.-.1.6.3.7.2.7.6.6.2.0...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.....813848.....D_....3N...W...9F.C....

C:\Users\user\Desktop\DFCE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	93153
Entropy (8bit):	7.835054103634326
Encrypted:	false
SSDEEP:	1536:oaxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncoclV1AWHP:olbr0o45GUgHhX8jC9ySogV1AWHP
MD5:	47C592EB97A153A45E1C51F969D8C787
SHA1:	9095E3626503E6B3F9FD173927A00FDDCB4B7234
SHA-256:	F779082667B29A95A2A60C3261C15C09BD80A414898FCFF2B1E7B528C940F8CD
SHA-512:	ED7A8E25541678B44242D5BCC5743F30CBAD3518E65E5DDE6A16FF61410450A1DD11B9A0365154B081F91CB539955C9C21191575CF365AD71E64D79A87C778E
Malicious:	false

C:\Users\user\Desktop\DFCE0000	
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\~$plan-1637276620.xlsm	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
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):	7.835274324451968
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	plan-1637276620.xlsm
File size:	93191
MD5:	4d44784f088b8dd2ac0a6cbf2b809eab
SHA1:	7d01c190b2e73c860a9aed904729c6466230bd26
SHA256:	c63e0b01a696a077a5709b8aa4d4d600344fc1ddba624cbd67c6f37f271d97ac
SHA512:	09c221b8d32ff3a0cb092789103d54ef64b1dffa92a1cdb7047436c6d9e578ee505457d327a55f1dac5f6b2bcd934c80b025b92b50da12ecdc3187e86efa6b69
SSDEEP:	1536:aY2xJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncW3SLBT0Ca:aYRbr0o45GUgHhX8jC9ySWCLBI
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 "plan-1637276620.xlsm"

Indicators

Has Summary Info:	
Application Name:	

Indicators

Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

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 13:27:19.948889971 CEST	192.168.2.22	8.8.8.8	0x6029	Standard query (0)	ieronymou.com	A (IP address)	IN (0x0001)
Jun 22, 2021 13:27:23.091567993 CEST	192.168.2.22	8.8.8.8	0xe1c4	Standard query (0)	iliknaturals.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 13:27:20.132361889 CEST	8.8.8.8	192.168.2.22	0x6029	No error (0)	ieronymou.com		192.185.21.116	A (IP address)	IN (0x0001)
Jun 22, 2021 13:27:23.157710075 CEST	8.8.8.8	192.168.2.22	0xe1c4	No error (0)	iliknaturals.com		103.50.160.62	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 13:27:20.536160946 CEST	192.185.21.116	443	192.168.2.22	49167	CN=ieronymou.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.	Wed Jun 09 05:35:43 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Tue Sep 07 05:35:43 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		

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 13:27:23.508169889 CEST	103.50.160.62	443	192.168.2.22	49170	CN=iliknaturals.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Apr 27 21:55:14 CEST 2021 Wed Oct 07 21:21:40 CEST 2020	Mon Jul 26 21:55:14 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2564 Parent PID: 584

General

Start time:	13:26:34
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:	0x13f870000
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: 2184 Parent PID: 2564

General

Start time:	13:26:45
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\wail1.dll
Imagebase:	0xff670000
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: 960 Parent PID: 2564

General

Start time:	13:26:46
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 ..\wail2.dll
Imagebase:	0xff670000
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