ID: 441941
Sample Name: diagram-1878769052.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:20:39
Date: 29/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

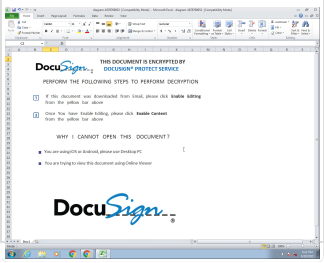
Windows Analysis Report diagram-1878769052.xls

Overview

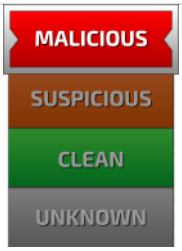
General Information

Sample Name:	diagram-1878769052.xls
Analysis ID:	441941
MD5:	5dc0dbb9a817db..
SHA1:	6e51ed7744080f5.
SHA256:	22c8c25451ead7..
Infos:	

Most interesting Screenshot:



Detection



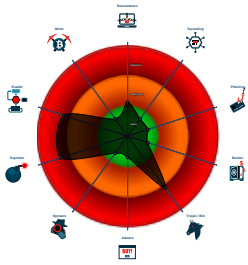
Hidden Macro 4.0

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- 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 …
- Outdated Microsoft Office dropper d…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2064 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - rundll32.exe (PID: 2460 cmdline: rundll32 ..\durio.fur,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
  - rundll32.exe (PID: 1616 cmdline: rundll32 ..\durio.fur1,DllRegisterServer MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
diagram-1878769052.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
diagram-1878769052.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Outdated Microsoft Office dropper detected

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

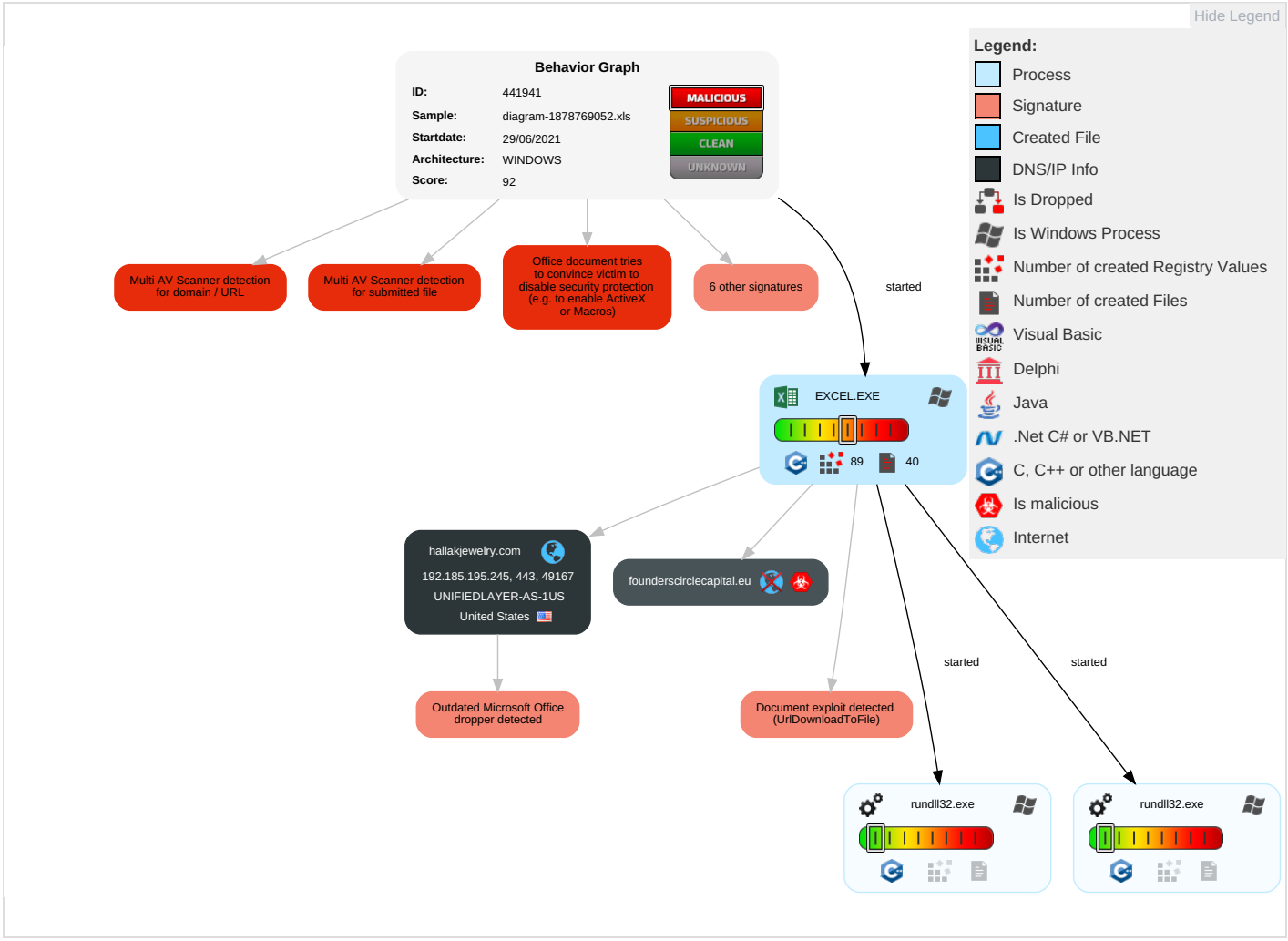
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

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	Im
Valid Accounts	Scripting 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory 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	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	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	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	Query Registry	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	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

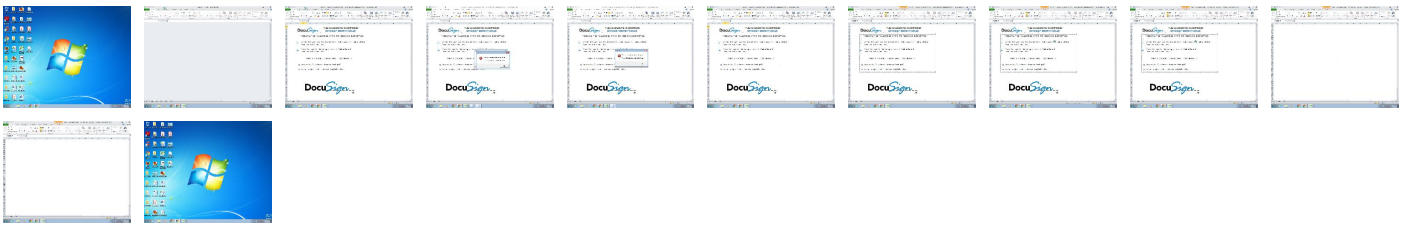
Behavior Graph

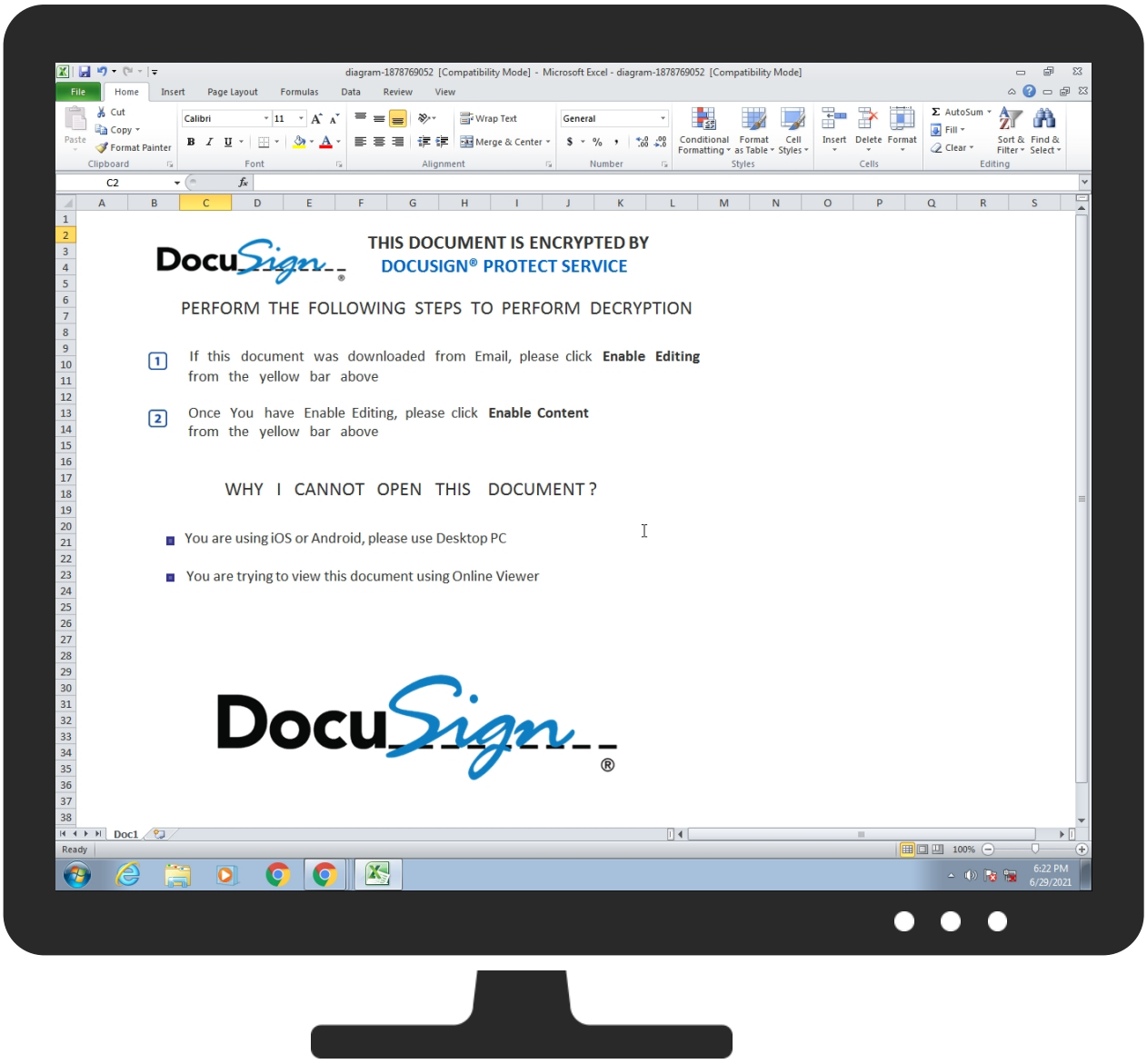


Screenshots

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
diagram-1878769052.xls	25%	Virustotal		Browse
diagram-1878769052.xls	38%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
hallakjewelry.com	3%	Virustotal		Browse
founderscirclecapital.eu	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hallakjewelry.com	192.185.195.245	true	false	• 3%, Virustotal, Browse	unknown
founderscirclecapital.eu	unknown	unknown	true	• 6%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.195.245	hallakjewelry.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441941
Start date:	29.06.2021
Start time:	18:20:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	diagram-1878769052.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:	8
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:	mal92.troj.expl.evad.winXLS@5/11@2/1
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: .xls • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.195.245	diagram-586589391.xls	Get hash	malicious	Browse	
	diagram-586589391.xls	Get hash	malicious	Browse	
	diagram-816901094.xls	Get hash	malicious	Browse	
	diagram-816901094.xls	Get hash	malicious	Browse	
	diagram-90301250.xls	Get hash	malicious	Browse	
	diagram-90301250.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hallakjewelry.com	diagram-586589391.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-586589391.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-816901094.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-816901094.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-90301250.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-90301250.xls	Get hash	malicious	Browse	• 192.185.195.245

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	statistic-1496367785.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1496367785.xls	Get hash	malicious	Browse	• 108.179.232.80
	4dvYb6Nq3y.exe	Get hash	malicious	Browse	• 50.87.238.189
	Remittance.xls	Get hash	malicious	Browse	• 162.241.120.180
	SecuriteInfo.com.Trojan.Win32.Save.a.27842.exe	Get hash	malicious	Browse	• 192.185.164.148
	SEOCHANG INDUSTRY Co., Ltd..exe	Get hash	malicious	Browse	• 162.241.24.206
	7R9igRpuL4.msi	Get hash	malicious	Browse	• 192.185.0.218
	nxinF8KuKS.exe	Get hash	malicious	Browse	• 192.185.16.56
	242jQP4mQP.exe	Get hash	malicious	Browse	• 50.87.248.20
	Halkbank.exe	Get hash	malicious	Browse	• 192.185.0.218

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HBenKsn2R8.exe	Get hash	malicious	Browse	• 96.125.162.104
	DC Viet Nam Order list 6-25-21.exe	Get hash	malicious	Browse	• 162.144.0.158
	Minutes of Meeting 22062021.exe	Get hash	malicious	Browse	• 108.167.156.42
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	factura y factura de la v#U00eda a#U00e9rea.exe	Get hash	malicious	Browse	• 74.220.199.6
	T5gtQGRL8u.exe	Get hash	malicious	Browse	• 162.241.135.156
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	statistic-1496367785.xls	Get hash	malicious	Browse	• 192.185.195.245
	New Purchase Order Air Shipment,pdf.pps	Get hash	malicious	Browse	• 192.185.195.245
	Scan8378 CTIMAIL3.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	BNK1135000001.docx	Get hash	malicious	Browse	• 192.185.195.245
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	PO20210628.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	PO 33015.doc	Get hash	malicious	Browse	• 192.185.195.245
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.18008.rtf	Get hash	malicious	Browse	• 192.185.195.245
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	PO20210624.doc	Get hash	malicious	Browse	• 192.185.195.245
	order-0798.doc	Get hash	malicious	Browse	• 192.185.195.245
	dridexxx.xlsb	Get hash	malicious	Browse	• 192.185.195.245
	vessel arrival notice.docx	Get hash	malicious	Browse	• 192.185.195.245
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 192.185.195.245
	sf0X1hMF0g.doc	Get hash	malicious	Browse	• 192.185.195.245
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	Bulk Order-0798.doc	Get hash	malicious	Browse	• 192.185.195.245
	PO20210624.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	Quote Requirment R2106131401 .docx	Get hash	malicious	Browse	• 192.185.195.245
	h2GeNTLcFz.xls	Get hash	malicious	Browse	• 192.185.195.245

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
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:	moderate, very likely benign file
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..:.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):	326
Entropy (8bit):	3.130754869956614
Encrypted:	false
SSDEEP:	6:kKKtACdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:+A+5kPlE99SNxAhUe0et
MD5:	69C681F66114FC037C20F40E1DA2AE65
SHA1:	134E31DC3ECC9D97CB9FAA9EC2CD7835CAB1CF47
SHA-256:	F6BFF33D6D0A1F1F2D99FC16A3514CB096CCC0E829A93A7ABC9220AB49F8091D
SHA-512:	7D1869E8283B8A9560103903BCB85E098B389B545A2ABEC4620B02BEA0D922A5CBF818EE2E836263D33D9FB6491BFF53C2C3E87512620BEC16BCADA38542E121
Malicious:	false
Reputation:	low
Preview:	p..... .....CRHNm..(..... .....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):	2.972124214357559
Encrypted:	false
SSDEEP:	3:kkFklAGIH1fllXlE/2S+HDHllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yR571:kK/fHy+HDXliBAIdQZV7QvB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
MD5:	417DFE5C5E14316E737D89D6D8666325
SHA1:	7FED29CB8F82477DCE62D34C7C31BD31A8A07950
SHA-256:	0180226412DB62BE910C520D175F6BDF9ABC3ECA80A239FD174894142F22B1D2
SHA-512:	04A871D10D82CEB6EF86DE849B000E04265828625F5A9121A9CB761DEB538AE23179A96342E9ADA7DE619427991968BE712577CCE3F63B32E3D0446B7B07C196
Malicious:	false
Reputation:	low
Preview:	p..... ....`....:.HNm..(..... .....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\Temp\52DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	82207
Entropy (8bit):	7.900890352254727
Encrypted:	false
SSDEEP:	1536:oJ6MCBI6qP16QCI/UyfqKdpkatlASfhWvHEGJXWy+W2G5xcU:oJ6iZP16QjJfVkZGhWvHEg7fxcU
MD5:	877BED76E1DD7795EE437DED290B0C5A
SHA1:	108A9AA94387BA2E55E82B9C88024E6F29E87247
SHA-256:	8AF988E732A6824339BDFA138FC97F3568335A084799CF42B00CE510743E620B
SHA-512:	7407ED0FBBAD30DA35C6E0FD0BD44A774DD7E225D8029635CBE14347B905AF3A84CDE94D9A1947E9F90FABDEBCD8A6D8216F478FB13560DC71FFCF6B70A2825
Malicious:	false
Reputation:	low
Preview:	.U.n.0....?.....(..r.izL.$...\K....I..V..p,;....vfvH...+k.G...k.Y3a.8.v].~.....pJ..ek@v1..iz....U;lY.R..9.....p4...D...A..O&....Ku..l6....`Ru....v...\|..Z&B0Z.DB..S;$._,....%..C....H.4!jb.w..5.....6k...+"..)..9..Pei.{.....C.y....0j....ZXr.....q9.~....fZ.a%.4.....s.4'.{Vx..T"/..#(..$../wR.Gt...Zqs..m.../.k.....~.]...x..}=.....~N.:..1.^DPw.b.{w..b..PQ<e.|xx....!^.....R,G8...D..u .l.6..%....t...|h(P{.y9.f.....PK.....!.[:.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabDC0E.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:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....\.....,.....I.....l.....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.|$....._Y..Y`&..s.1.....s.{.,."':o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.`=*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...l.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f\|.*...'^K`\..e.....j/..\|..)..&i...wEj.w...o..r<.$.....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\TarDC0F.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

C:\Users\user\AppData\Local\Temp\TarDC0F.tmp	
Reputation:	moderate, very likely benign file
Preview:	0..l...*.H.....l.0..l....1.0...`.H.e.....0..\...+.....7.....\.0..\.0...+.....7.....\.0..\.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=Mon May 31 00:21:39 2021, atime=Mon May 31 00:21:39 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.485643869027758
Encrypted:	false
SSDEEP:	12:85QfLgXg/XAlCPCHaXtB8XzB/CXX+WnicvbybDtZ3YilMMEpxRljKcTdJP9TdJPe:854/XTd6jUYeaDv3qFrNru/
MD5:	3483AE2443079359B9A347929F82F315
SHA1:	8123E694DCD2073161DF65B46D620FA562E2E01D
SHA-256:	004A15D50054E6F0F0AD763A1CB79D076F0D67F120CE59815BB2870962DE80ED
SHA-512:	0ED298F528EC70FED89FBBD4B5D14BCDAFC62442DFE081D97762426A775C834EE1D02145AAE01F8E8373FE1C0AF539BB60AA1578DA4E59454B8972C42BCCD6 34
Malicious:	false
Preview:	L.....F.....7G.....FNm.....FNm... .....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....Desktop.d.....QK.X.R..*..._=.....:.....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\..#.....\\648351\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.....648351.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\diagram-1878769052.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=Mon May 31 00:21:39 2021, atime=Mon May 31 00:21:39 2021, length=171520, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.540141172853911
Encrypted:	false
SSDEEP:	48:84/XT0jFSW+iqYFQh24/XT0jFSW+iqYFQ/:84/XojFSxLYFQh24/XojFSxLYFQ/
MD5:	BE3609777A62E3D0131E311396DB71A9
SHA1:	2B8BB8F399B92497F2F790B52928DD0A2F238A3B
SHA-256:	E9B509570D0CA783F2B56355D3264752989FB88F76CFC32A37A0C25D644A1BEF
SHA-512:	256A5A48CEA078D0D6FB834B32F369B9477F8916892188F6F1E7583E20929B6DBF03CD33907575BF0E1C54A05E921B08BFB51D191FB4CD8F56E77D73BBFFFEA2
Malicious:	false
Preview:	L.....F.... .....{.....FNm..QZ.FNm.....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.....v.2.,...R.. .DIAGRA~1.XLS..Z.....Q.y.Q.y*...8.....d.i.a.g.r.a.m.-.1.8.7.8.7.6.9.0.5.2...x.l.s.....-...8...[.....?J.....C:\Users\..#.....\\648351\Users.user\Desktop\diagram-1878769052.xls.-.....\....\....\....\....\.D.e.s.k.t.o.p.\.d.i.a.g.r.a.m.-.1.8.7.8.7.6.9.0.5.2...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.....648351.....D_....3N...W..

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):	107
Entropy (8bit):	4.851195869560029
Encrypted:	false
SSDEEP:	3:oyBVomMXCUUkQN6lZFdUkQN6lmMXCUUkQN6lv:dj6XCvkQS8kQ6XCvkQy
MD5:	027E2AFCDD06DD3DF9CC94970FC294A4
SHA1:	C1F15C35ADF3EA115CA99740EEF8927F35C05154
SHA-256:	94AC427E287B5A0C4A4017D90BAB2D66485AC0A211640CA0CDD0687CB087CC93
SHA-512:	4456E497CCAD37068DA4AB5C12F547B1D36B749823F48674466565B92E7C927B1F830574BD51691B66B84136097D413B916E038F5BF09C8D4FB70C2D3CDB954A
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..diagram-1878769052.LNK=0..diagram-1878769052.LNK=0..[xls]..diagram-1878769052.LNK=0..

C:\Users\user\Desktop\13DE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16

C:\Users\user\Desktop\13DE0000	
Category:	dropped
Size (bytes):	202692
Entropy (8bit):	5.607314959839426
Encrypted:	false
SSDEEP:	3072:1D87P1vQjFfVkdGeW5fGVTPw+zvWnb+quX/DXPXrwP/D8jP1:GP1mfV0jwPYP1
MD5:	6FE7FC3E4F839E9418548463AA359185
SHA1:	95BD665198FF41FC4D708635916644E41715975E
SHA-256:	84AC527EAB0B0AB66AF622222F960AF59ACC382601053EC1D771C37C784BC8F1
SHA-512:	C8D82D880B38B08934A710EC4F06849C6C2E59FDCD74FF3A3798328FFA4033133A73C981A07AC33230162E6FD6D13225DFE58A608ACACEE0B133AE012CAD0F F
Malicious:	false
Preview:	........g2.....\.p....user B.....a.....=.....=.....i..9..8.....X.@.. ....."....1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1..h...8.....C.a.m.b.r.i.a.1...,...8..... .....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....8.....A.r.i.a.l.1.....<.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....4.....A.r.i.a.l.1.....C.a.l.i.b.r.i.1.....A.r.i.a.l.1 .....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....?.....A.r.i.a.l.1.....A.r.i.a.l.1 .....A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Grog, Last Saved By: Grog, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu May 20 08:01:36 2021, Security: 0
Entropy (8bit):	2.078617301736935
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	diagram-1878769052.xls
File size:	535552
MD5:	5dc0dbb9a817db4a5f589f670c6b9241
SHA1:	6e51ed7744080f5583beb20fd7052e2fcbf7cd3a
SHA256:	22c8c25451ead7742914a869f775af6e8751907a83b4607 7b8439d03a9105c81
SHA512:	ee37b3b4c2ba204b542a091104bda6f1a0097a17e131a7 9edf48f7fe3941d36df248bfd0c2dcc4c7d075abdc827306 68587fa68e739175d58c0b5e9688edb260
SSDEEP:	1536:pq35xFlHVRl1X/7fi18snt52U20kyti4kmhRd+s2teb Lxtf7t69KRGF:pq35xFl1Rl1Pas+ilmhR4s2tQVtfgDF
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "diagram-1878769052.xls"

Indicators

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

Indicators

Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1251
Author:	Grog
Last Saved By:	Grog
Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-20 07:01:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Contains Dirty Links:	False

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 29, 2021 18:21:32.060880899 CEST	192.168.2.22	8.8.8.8	0x7e45	Standard query (0)	hallakjewelry.com	A (IP address)	IN (0x0001)
Jun 29, 2021 18:21:34.557127953 CEST	192.168.2.22	8.8.8.8	0x5410	Standard query (0)	foundersci rclecapital.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 29, 2021 18:21:32.255386114 CEST	8.8.8.8	192.168.2.22	0x7e45	No error (0)	hallakjewelry.com		192.185.195.245	A (IP address)	IN (0x0001)
Jun 29, 2021 18:21:34.613322973 CEST	8.8.8.8	192.168.2.22	0x5410	Name error (3)	foundersci rclecapital.eu	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 29, 2021 18:21:32.627311945 CEST	192.185.195.245	443	192.168.2.22	49167	CN=hallakjewelry.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.	Sat May 15 06:53:35 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 06:53:35 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: 2064 Parent PID: 584

General

Start time:	18:21:36
Start date:	29/06/2021
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:	0x13ffc0000
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: rundll32.exe PID: 2460 Parent PID: 2064

General

Start time:	18:21:42
Start date:	29/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\durio.fur,DllRegisterServer
Imagebase:	0xff720000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 1616 Parent PID: 2064

General

Start time:	18:21:43
Start date:	29/06/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32 ..\durio.fur1,DllRegisterServer
Imagebase:	0xff720000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
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