ID: 438525
Sample Name: tender-1235416393.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:51:20
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

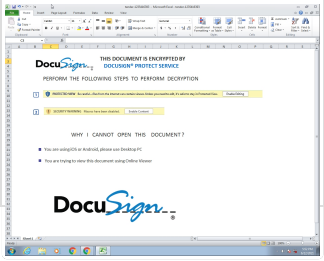
Windows Analysis Report tender-1235416393.xlsm

Overview

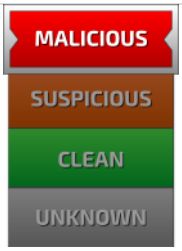
General Information

Sample Name:	tender-1235416393.xlsm
Analysis ID:	438525
MD5:	7b3bc7d505fcb3b..
SHA1:	aea1e832eed27f0.
SHA256:	bfe0e882d0ca0fb..
Infos:	

Most interesting Screenshot:



Detection



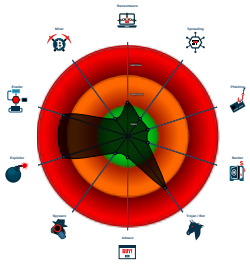
Hidden Macro 4.0

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for doma…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Yara detected MalDoc1
- Excel documents contains an embe…
- IP address seen in connection with o…
- Internet Provider seen in connection…
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2156 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - regsvr32.exe (PID: 2784 cmdline: regsvr32 -s ..\erty1.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2700 cmdline: regsvr32 -s ..\erty2.dll MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
sharedStrings.xml	JoeSecurity_MalDoc_1	Yara detected MalDoc_1	Joe Security	
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	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

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

Yara detected MalDoc1

System Summary:

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

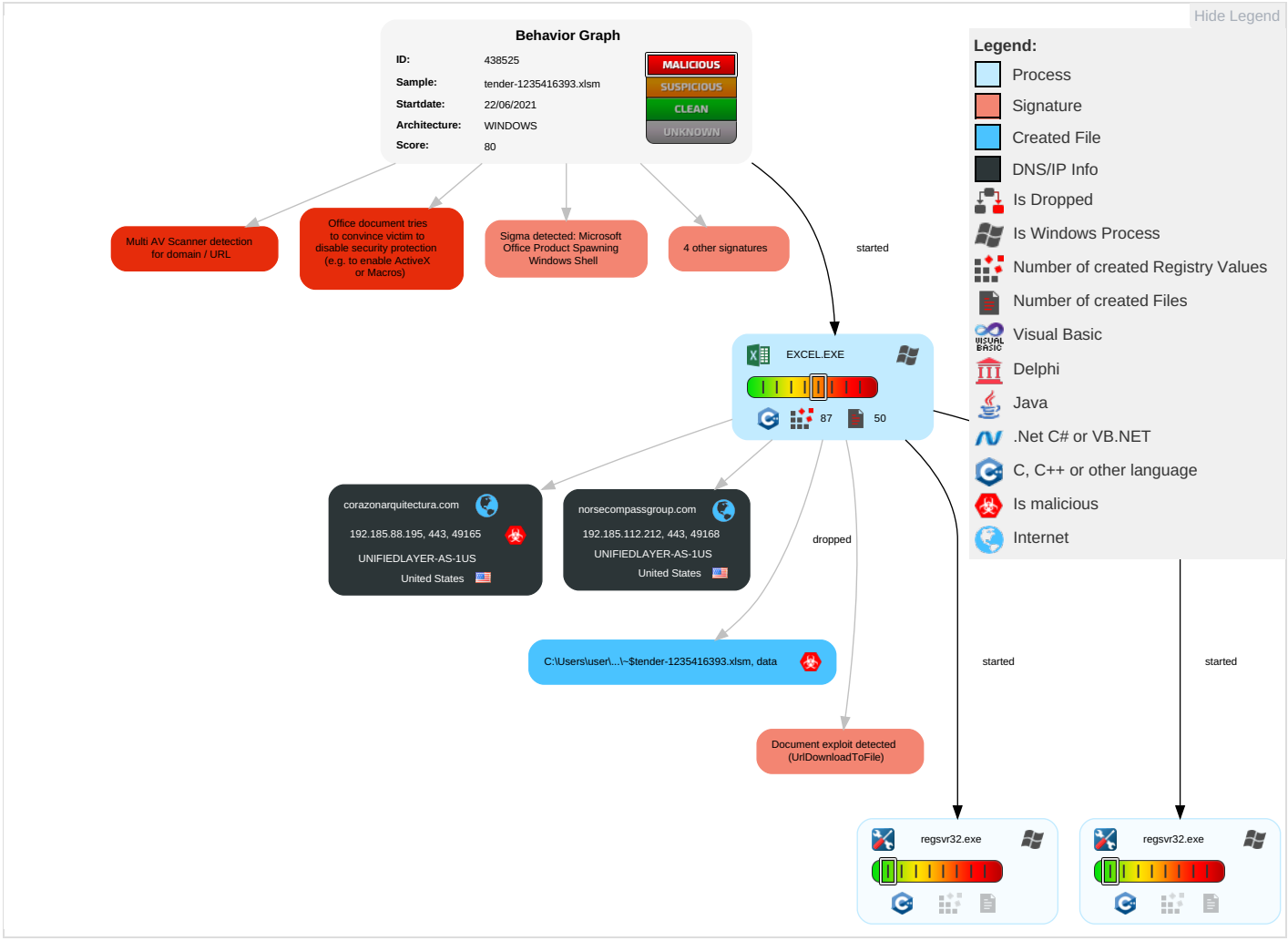
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Scripting 2 1	Path Interception	Process Injection 1	Regsvr32 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
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Masquerading 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 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
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	Ingress Tool Transfer 1	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

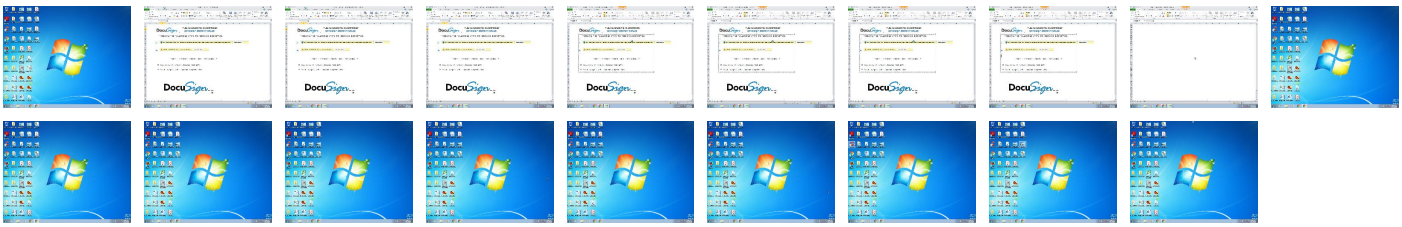
Behavior Graph

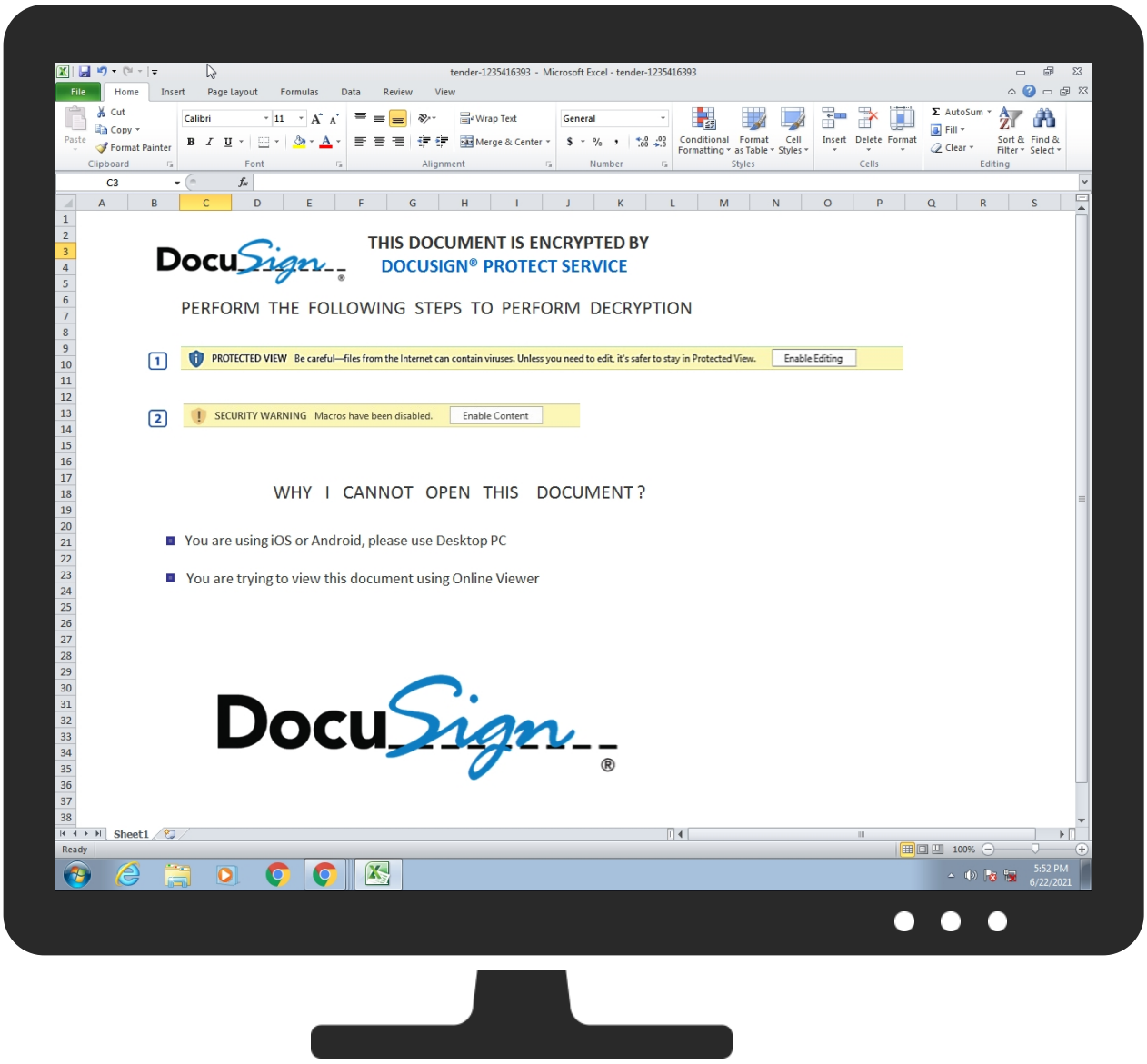


Screenshots

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

Source	Detection	Scanner	Label	Link
norsecompassgroup.com	0%	Virustotal		Browse
corazonarquitectura.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
norsecompassgroup.com	192.185.112.212	true	false	• 0%, Virustotal, Browse	unknown
corazonarquitectura.com	192.185.88.195	true	true	• 7%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.112.212	norsecompassgroup.com	United States		46606	UNIFIEDLAYER-AS-1US	false
192.185.88.195	corazonarquitectura.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438525
Start date:	22.06.2021
Start time:	17:51:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tender-1235416393.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:	6
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:	mal80.troj.expl.evad.winXLSM@5/18@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 • 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
192.185.112.212	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	
	tender-156639535.xlsm	Get hash	malicious	Browse	
	tender-156639535.xlsm	Get hash	malicious	Browse	
	tender-2038988342.xlsm	Get hash	malicious	Browse	
	tender-2038988342.xlsm	Get hash	malicious	Browse	
	sentence-1711450431.xlsm	Get hash	malicious	Browse	
	sentence-1711450431.xlsm	Get hash	malicious	Browse	
192.185.88.195	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	
	tender-156639535.xlsm	Get hash	malicious	Browse	
	tender-156639535.xlsm	Get hash	malicious	Browse	
	tender-2038988342.xlsm	Get hash	malicious	Browse	
	tender-2038988342.xlsm	Get hash	malicious	Browse	
	sentence-1711450431.xlsm	Get hash	malicious	Browse	
	sentence-1711450431.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
norsecompassgroup.com	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	tender-156639535.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	tender-156639535.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	tender-2038988342.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	tender-2038988342.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	sentence-1711450431.xlsm	Get hash	malicious	Browse	• 192.185.112.212
	sentence-1711450431.xlsm	Get hash	malicious	Browse	• 192.185.112.212
corazonarquitectura.com	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-156639535.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-156639535.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-2038988342.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-2038988342.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	sentence-1711450431.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	sentence-1711450431.xlsm	Get hash	malicious	Browse	• 192.185.88.195

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
UNIFIEDLAYER-AS-1US	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	TT_COPY.MT103.SWIFT.docx	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	MT103.docx	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	Purchase_Order.doc	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.19092.rtf	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	aim-1860610262.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	otKl5DLaUo.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	bKYGBZ8BPl.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-1127603629.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-1134058065.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-1132671574.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-1128721882.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-108527315.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	idea-112755060.xlsm	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	viru.xls	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	viru.xls	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195
	JPM Chase Remittance Advice.xlsx	Get hash	malicious	Browse	• 192.185.112.212 • 192.185.88.195

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:O78wlEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Reputation:	moderate, very likely benign file

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

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1263750649191113
Encrypted:	false
SSDEEP:	6:kKNchse8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:Whs8kPlE99SNxAhUe3OMx
MD5:	33F70B57FE702E8EB6A74856FB1765BC
SHA1:	5CC043EAE2355747348DDE9D1B437D24905FCD24
SHA-256:	7D7B2817B2B5C838E7ED5296F2601B7DB3D6EC4E641D3F1EE76AC8C1AFD86BCC
SHA-512:	56AA25F5E8876650221EC16245F5A89A7EE802386385D09ACE73511330BA281CA0CA914DA67E9FF698A3B3229201BB5BEA3C0B940DE8827A3145D87FDF917934
Malicious:	false
Reputation:	low
Preview:	p..... .....L...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):	2.9879972302305746
Encrypted:	false
SSDEEP:	3:kkFkltsCftfllXlE/2S+HDHllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1yR571:kKWjfq+HDXliBAIdQZV7QvB
MD5:	C0B83C50F5EB0932F89FF3749B61E576
SHA1:	33F47F463C6F56C16A94F5815D012ED6357A89E6
SHA-256:	B8312CFCAF62C111962F6FC14D63170043415682D1B0D3F6458E3C2CEE9BAA5A
SHA-512:	861D62A5C112B50DC519AD3E22CD01921ADC29122BC650A35D05F16B820FC08CAFC013A5CCE41804AEC9EE6001968BDDE8DC69581F6E70B3FFD5C584A7026I 9
Malicious:	false
Reputation:	low
Preview:	p..... ....`...*i...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\375F21A2.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 521 x 246, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\375F21A2.png	
Category:	dropped
Size (bytes):	32996
Entropy (8bit):	7.975478139053759
Encrypted:	false
SSDEEP:	768:N4k48AnTViUidx37OODgvnrxtxAudMN1VTRVHdB4K7K:NE8m+L37OOwrCXN1VTR1PK
MD5:	4E69B72B0CE87CC7EE30AA1A062147FE
SHA1:	09B0AA5414E08756E0AE53E1BE5C70DB4DEAF2E8
SHA-256:	77A1F749389CBF771D5197FF0FF17113FCA1D91989ADCADF2852876A6CC14988
SHA-512:	6246AF2137E773F7719033AFE75F0B00FF3A4B5543DBA53737FC8D33EE42478E3D8A5CF166E9EFD2F54A2F3E0D62417BDDC1CB824642305B59AB1229313D2D7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....[.J....sRGB.....pHYs.....+.....IDATx^.].`.....{%.$..A...R.P@z....O...S.<;.VT.REA.(...I...{.....m...]..r./.....~.|]h.Z....P.(.....E."@...P.(.v.P.@..E."@. ...#@y.....E."@y.....E."...*78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...)..... !@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P ..!@y.3.....E....."@...8C...g...)......!@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3 ..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...)......!@y..9.1E."@.p.....S.(....C....[s:c..E."......!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5E32AA01.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 246 x 108, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	10270
Entropy (8bit):	7.975714699744477
Encrypted:	false
SSDEEP:	192:3sXvKLMbye/PEXiKTUgCto9h4F6NwfU6vGDpdYNbcQZgkbd4cgc:3iLh/gJ59CDfU6LocbGK
MD5:	9C4F09E387EA7B36C8149EA7C5F8876E
SHA1:	FF83384288EB89964C3872367E43F25FAFF007CC
SHA-256:	A51C1D65092272DAEB2541D64A10539F0D04BC2F51B281C7A3296500CFCA56DE
SHA-512:	0FDDE22CFDDE8BB1C04842D2810D0FD6D42192594E0D6120DE401B08B7E2CFFB5333792BC748E93CD70FA14734CC7D950620CB977DDBBDB52D92BDA8F3552 F8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....I.....sRGB.....pHYs.....+....'.IDATx^.].|.U...%...J."....H.&Ui.....E.....D.7....U.i..FH#=.....3..$K...'{3....7.....0.H.....H..03..,....8.q.....'@\. ..S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8..... .`..) @...X...q..>N...>.....q.....'@\...S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8...I..m.i'Sj.W.i.S.TJ....D.D._%...] ..i.;J..b..T.).Ik.L6..L.mN....!*..\..'{$.o._b..h....t"@.?...y...d..h..|..B9D..CJD..t."......bR"....I)H....z.....>|.....E.x..r....J.U..[...p:D....XF.....A...E.....b..C...C..C.....=.Z..$.=../....Y ..x5CY.0l..,~.W. .?.....;...$.'....<.H.2...z..6(.E.....kw8w^.\~...".C,gl&.m..J2.).HI.....b.r...'.....r.H...P....'...A.^.q..j).cZ.^1~.|.....dv^.^v..X..v..6/^.$rR. iK..H.Uu.Pvk....U.....'.Fd..Z .]mu*1.Zb.\b...N..P..&tr;.W....J.K(@.^A..R.S.[~.v.R.YO...0-...2..h."..............7..Ng...R...e.&..@..t..N...{5...W.x./#.%..}t...F8-..M1..(4b1....&.....)B...6.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9268080E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 934 x 29, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	42557
Entropy (8bit):	**7.992800895943226**
Encrypted:	**true**
SSDEEP:	768:Pfsq4UmepRdblCFcXhw9KnRTRews6xD0FvBlwAS1A8x7BcS0OvD230:PR3ZblCF28KRsws6CFv0AYx7Bl3b230
MD5:	B1F262A694930ADB699FA94E3394887F
SHA1:	9C9B66D3A3F09AECA45DB94304CDD6FB3C5BD4C9
SHA-256:	9C99EC61392B9022A38C1354124360147E8185065095BD2EC92B1416CF9F4B68
SHA-512:	1CA7E6750178B88EC3AA7A0B83348EA389E26C27E0D7E919D807BE470714E5B4F04ACEB69D391F0498D4E465E6620E9449CA2F40755B5CE8196E683502EBF5F4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....6.....sRGB.....pHYs.....+.....IDATx^....dU....S.:ON.0.0....s0 .....$..%#HR.T.....$..0C...Su...[.TM..{.....C.S}..^{.....].^..ZX.Wb.W....X!..A.P... .0..u...X.V.3.....z..tiO{GW..?...A.....ca2Y.... ...cAX..zZ..2M.$..g.O.e..r?z&.....*....*.=..Z.A.....a.Z..ka<..N.R.c...../.[..j.^...Nk.(..y.,..z"...R..Z+..D1Q....z....0..u~. .jU_.b.Z.V....:..5:.(.....-...A2.O.{..p.j..].<.....0..0..+...E...^...z....#..j.d...X._..1..M.5..O.^.."..I....G....U1.....X.6.Z.\.&..h..m*..T..xH.j..3<$.H...a..n....}t.A.jT.6G.h@..<.x..x...cb.. ....C..{.D.'QW<.o~..?.....4F_...B..h.\...y8..)....j.Z.d..#P..P..O.....(.0...f....B_z>.E .w../..(...'.Fw..yT..G..)...b9..g.AA`.a..v.zfY.F......._r.i.d.`....Q.g.m"..\..&.t.X.q1}.$.S....2..~...d."..1.. (.0.F....t...i..@f.. ...(..8..q.....I.....ad.....z%....;...y.O...X<Q..X.....B..H.....<)....4.&9.4.....1.h..#B.....g.....bO.59.A..M.....J..vX3*5..X....(G.A.u...8.. .{

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A76CD200.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A76CD200.png	
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ lr.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;...X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._.j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\ABDBFCB7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 490 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	18547
Entropy (8bit):	7.9850486438978985
Encrypted:	false
SSDEEP:	384:kBCIQCloAwCZDy0xOTn6/g6l4NpWfw9nHk6Ka01f7Y/H:kBCIQpAwODPMT6/gfOUKN70
MD5:	ED31C7053D581EDC4C98D222CE02EDEF
SHA1:	6BA7A49CC6FF8FE00E9C5BC75F48AB7E679536DD
SHA-256:	0FCF61397154DF01CFAECA362BD643D88AAD5FEDD07B52DC8A921CC0D7236534
SHA-512:	929BF13F2A050B33D0EABDAC97CAAFDDE612AD521027FEE4DD51E28A3CF61198D6C045E00AB85223C73D74D18BB4EAA1681C7AFA917946DC08A3C75FB2AB4 935
Malicious:	false
Preview:	.PNG.....IHDR.....l{.....sRGB.....pHYs.....+....H.IDATx^...U....."x....U...."...Tc.{...M1M..In....TATb4F,`oD..Q..3.....g.3..Lr.D....a8....~.z....Z...yyF..9...:.H .Q2..)/L.....Q.}....(J.,...w2>R.$..G2..m>..|...0.M.g.Xnjj...P.v..x....S.....B..p.=.Lz.^..Wi..2U.V'.a..*DE.'..rT.z....#.;..]....[?.C...o.m`]..m][;.:<..]F.9..u..Q]c.Ue.9....(.F.Z.~s..Q:..B.. .)..LZ.TTo..P.gc.l.'.X.}..H....Q.h|....L..rcd.2dN..co..5.....w.U.4..}.....{.Q.....D2.J.z~..:Y3,.H..(#.J.Q.....N.._7....w.....].2w.6...._....u.....9-.7.f9...E9...p.A..f....=....Bqu....A .u.JG>b"...%..0..W.H=...G#.DR.....P.|FD).NJ....)>.;...M...T*.dW..t:[.xT..M.|S...O..."M.4u7.uS...]4..R.vK....*).ZK.. J.=.9C.].kr..ES..6..f.(.....N':..t..^.S....kn[s.#..(.....m.....~....6>.... :u.J.mO.....%D...Q...6%....!.....H.....v..^%....$._..V.....[o5.H8.....n.~M.z.RL.0p:.iC.k.1..$.....3[....mS5.....E...2.&...k]...A.....K.8...5..O.@7.[-.F4*7...i....in...y....A

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D413B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.]..........O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Temp\51EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	183962
Entropy (8bit):	7.960424128267181
Encrypted:	false
SSDEEP:	3072:GOlCxAVIKF9zw3g2dH8UOP9VlUBWA6CFvA7bXqluQDJ/0isixVymd1xXPUHw:GOMYFp3liWA6Fel1J9sixVyWxfT
MD5:	6EB574AE48A728B8764CA607B9A21C79
SHA1:	7C420DAB4E47CE53150EE5E02032A100A913AD56
SHA-256:	782E66BD5958E789B3908998816A26D68484E4FDAECA6946535115FA4DC3D0F1
SHA-512:	45E629A347ED03E4FC66681F5C56D34C506847352B1DD50D2BFC8F5E262B3C1DC79B0C19C24E7AEA988032B6BB6240EB2BCE8CAAE1205A51517E90FD2A70D6 E8
Malicious:	false

C:\Users\user\AppData\Local\Temp\51EE0000	
Preview:	.U.N.0..#....(qa1.....%.....}.X.K....k7..JC...<..=.o..+k.G...k.y3a.8.v]..._.?Y.I8%.w.5 ....L....")._.....I|.G3...H..;..\....d.K...T...f.?...&UW+..8.k...T.D.FK..(.tjG.....|.D.`. ....&DM ...R....u;..f.y|?"....!.....u.3....<.~../-`...[...._....r...9L..X.J.iJb..2.+'..hNh....RA"/...H..$../WR...q.M>J~C ...C.CF...../..'_hF.1.....!.S.E.u..@w_n.5.....S.....>....v.}@j...O...dt...b..> ...V...;=.r{W..h..;.....PK.....!...g.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\CabED1E.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:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789AB EB
Malicious:	false
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|||.w.M.!<- .}%.C<tDX5\s._..I..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...I...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.I..`D..e.i`....y....,.5....aSs`..W...d...t.J...]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

C:\Users\user\AppData\Local\Temp\TarED1F.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...210519191503Z0...+......0..T.0..*.....`...@.,..0..0.r1...0...+.....7..~1......D...0...+.....7..i1...0 ...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a. t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....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 23:51:43 2021, atime=Tue Jun 22 23:51:43 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.501343027271025
Encrypted:	false
SSDEEP:	12:85QJlLgXg/XAlCPCHaX2B8GB/jkZX+WnicvbhnbDtZ3YilMMEpxRljKBTdJP9TdU:85Y//XTm6GkYeNDv3qErNru/
MD5:	756FF46FB3F6D80E9493DF1833A7A06B
SHA1:	DA8B81668833B9F034152FA256A62CFE1B5F7C85
SHA-256:	9122523DBC291905E702D13859C1CBEB3A2D5EE29F85D6E54AF9490F818BF0D0
SHA-512:	4806DE18CBCE28031FA6FD823E5E80FFE891BBC8FC343C3F8ECCA92BE7D2A262FB37FB2A1F0A1CF7A548405D8FA83BA3F25C52764FC0C56EF2004BEC30AC9 11
Malicious:	false
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.....Rv...Desktop.d.....QK.X.Rv.*..._=.....:.....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\..#.....\\992547\Users.user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:..,.LB.)...Ag.....1SPS.XF.L 8C....&.m.m.....-..S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....992547.....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):	106
Entropy (8bit):	4.763212817751883
Encrypted:	false
SSDEEP:	3:oyBVomxWawOwWLUlJwOwWLUlmxWawOwWLUlv:djX32V3z32
MD5:	B4F6BB060CA7FE2606599338C05D24F5
SHA1:	C466F0DF355EA0D4C96932C35460BA305862DC5F
SHA-256:	46263D33B06608B58D3824D8C3F25B6254B46AED55B0157B0EB013DB5D5E2C41
SHA-512:	DF4FD9CD6523704CA2B1E6A1E4D93A583D5936D7B1F50D681AA4782180C5871A05D40AC460C9D1C3126D4A1A70A24ACD8C8446BB1629CC0EB6AD6FD7B639E8
Malicious:	false
Preview:	Desktop.LNK=0..[misc]..tender-1235416393.LNK=0..tender-1235416393.LNK=0..[misc]..tender-1235416393.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\tender-1235416393.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 14:08:18 2020, mtime=Tue Jun 22 23:51:43 2021, atime=Tue Jun 22 23:51:43 2021, length=183962, window=hide
Category:	dropped
Size (bytes):	2108
Entropy (8bit):	4.54162683913729
Encrypted:	false
SSDEEP:	24:8/Ju/XTm6GreVIEeVQrDv3qEdM7dD2/Ju/XTm6GreVIEeVQrDv3qEdM7dV:8k/XTFGqVw/EQh2k/XTFGqVw/EQ/
MD5:	A6BF9FE9AF4D155994B9C87CEBA5024C
SHA1:	53B9AA7FF737A5309F9E03C790154FD40AFEBCCD
SHA-256:	0D354447AFDC923C2BA1DCC49DA29F35BCAB705A4108296403D7B501CBFA1D21
SHA-512:	08F441A226B901B9CF2CB301E10CC240004C6DA7967A96E295941AC77EC8C5786E85947BCE5875E323E40F6F347F1178E9010E091F95131E02B70A406C903B8B
Malicious:	false
Preview:	L.....F.... .....{...~]..g..#.k..g.....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.....Rs. .TENDER~1.XLS..Z.....Q.y.Q.y*...8.....t.e.n.d.e.r.-.1.2.3.5.4.1.6.3.9.3...x.l.s.m.....-...8...[.....?J.....C:\Users\..#.....\\992547\Users.user\Desktop\tender-1235416393.xlsm.-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.t.e.n.d.e.r.-.1.2.3.5.4.1.6.3.9.3...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.....992547.....D_....3N...W..

C:\Users\user\Desktop\92EE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	183962
Entropy (8bit):	7.960424128267181
Encrypted:	false
SSDEEP:	3072:GOlCxAVIKF9zw3g2dH8UOP9VlUBWA6CFvA7bXqluQDJ/0isixVymd1xXPUHw:GOMYFp3liWA6Fel1J9sixVyWxfT
MD5:	6EB574AE48A728B8764CA607B9A21C79
SHA1:	7C420DAB4E47CE53150EE5E02032A100A913AD56
SHA-256:	782E66BD5958E789B3908998816A26D68484E4FDAECA6946535115FA4DC3D0F1
SHA-512:	45E629A347ED03E4FC66681F5C56D34C506847352B1DD50D2BFC8F5E262B3C1DC79B0C19C24E7AEA988032B6BB6240EB2BCE8CAAE1205A51517E90FD2A70D6E8
Malicious:	false
Preview:	.U.N.0..#....(qa1.....%.....}.X.K....k7..JC...<..=.o..+k.G...k.y3a.8.v]..._.?Y.I8%.w.5 ....L....")..._.....l|.G3...H..;..\....d.K...T...f.?...&UW+..8.k...T.D.FK..(.tjG.....|.D.`. ....&DM ...R....u;..f.y|?".....!.....u.3....<.~.../.`...[....._....r...9L..X.J.iJb..2.+'..hNh....RA"/...H..$../WR...q.M>J~C ...C.CF...../..'_hF.1.....!.S.E.u..@w_n.5.....S.....>....v.}@j...O...dt...b..>...V...;=.r{W..h..;.....PK.....!...g.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$tender-1235416393.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

C:\Users\user\Desktop\~$tender-1235416393.xlsm	
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):	7.9629175676293995
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	tender-1235416393.xlsm
File size:	184537
MD5:	7b3bc7d505fcb3b4c0b30aeb3ee9d0a1
SHA1:	aea1e832eed27f02e48248cee5334bc1d20f1263
SHA256:	bfe0e882d0ca0fb04757d96181db67c3c5b67e636ac1e92b2d6f6b63e35f0097
SHA512:	5ff2b72e3dc9b8d2d76c8d10eae283e7cb6b130facbb27a840ea4e5c6ff5480ffe2396de84da07e15b8662cbc8fac658677f15a136ca98b3c4d47997a091309e
SSDEEP:	3072:IpV04Yldz+3qcyFaalxV+93qt6GtxVymd1xXPMU9VlUBWA6CFvA7bRCxAVIK0hKF:IpW4HCaalxV23qIYxVyWxfMU3liWA6Fb
File Content Preview:	PK.....!...g.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e2aa8aa4bcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "tender-1235416393.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:	

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 17:52:17.346479893 CEST	192.168.2.22	8.8.8.8	0xfda2	Standard query (0)	corazonarquitectura.com	A (IP address)	IN (0x0001)
Jun 22, 2021 17:52:20.217926979 CEST	192.168.2.22	8.8.8.8	0xf774	Standard query (0)	norsecompassgroup.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 17:52:17.531212091 CEST	8.8.8.8	192.168.2.22	0xfda2	No error (0)	corazonarquitectura.com		192.185.88.195	A (IP address)	IN (0x0001)
Jun 22, 2021 17:52:20.408560038 CEST	8.8.8.8	192.168.2.22	0xf774	No error (0)	norsecompassgroup.com		192.185.112.212	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 17:52:17.905528069 CEST	192.185.88.195	443	192.168.2.22	49165	CN=corazonarquitectura.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 17:53:50 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 17:53:50 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		
Jun 22, 2021 17:52:20.749152899 CEST	192.185.112.212	443	192.168.2.22	49168	CN=*.norsecompassgroup.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Tue Jun 08 16:06:25 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 06 16:06:25 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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: 2156 Parent PID: 584

General

Start time:	17:51:40
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:	0x13ff80000
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: 2784 Parent PID: 2156

General

Start time:	17:51:47
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\erty1.dll
Imagebase:	0xffc70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2700 Parent PID: 2156

General

Start time:	17:51:48
Start date:	22/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -s ..\erty2.dll
Imagebase:	0xffc70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis