ID: 510734
Sample Name: protocol.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:38:13
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

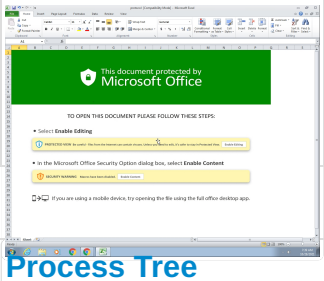
Windows Analysis Report protocol.xls

Overview

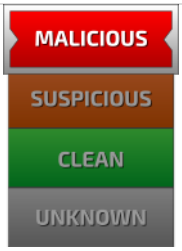
General Information

Sample Name:	protocol.xls
Analysis ID:	510734
MD5:	93383a84bdf0f5f…
SHA1:	455bb88e45935d..
SHA256:	ca641647b3e210..
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection



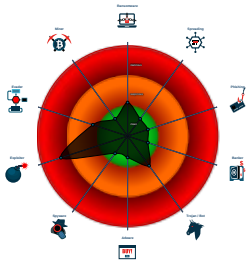
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for doma…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Internet Provider seen in connection…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 196 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2632 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2792 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2128 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
protocol.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x126aa:$s1: Excel • 0x1378f:$s1: Excel • 0x3610:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A
protocol.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\protocol.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x126aa:$s1: Excel • 0x1378f:$s1: Excel • 0x3610:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\protocol.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

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

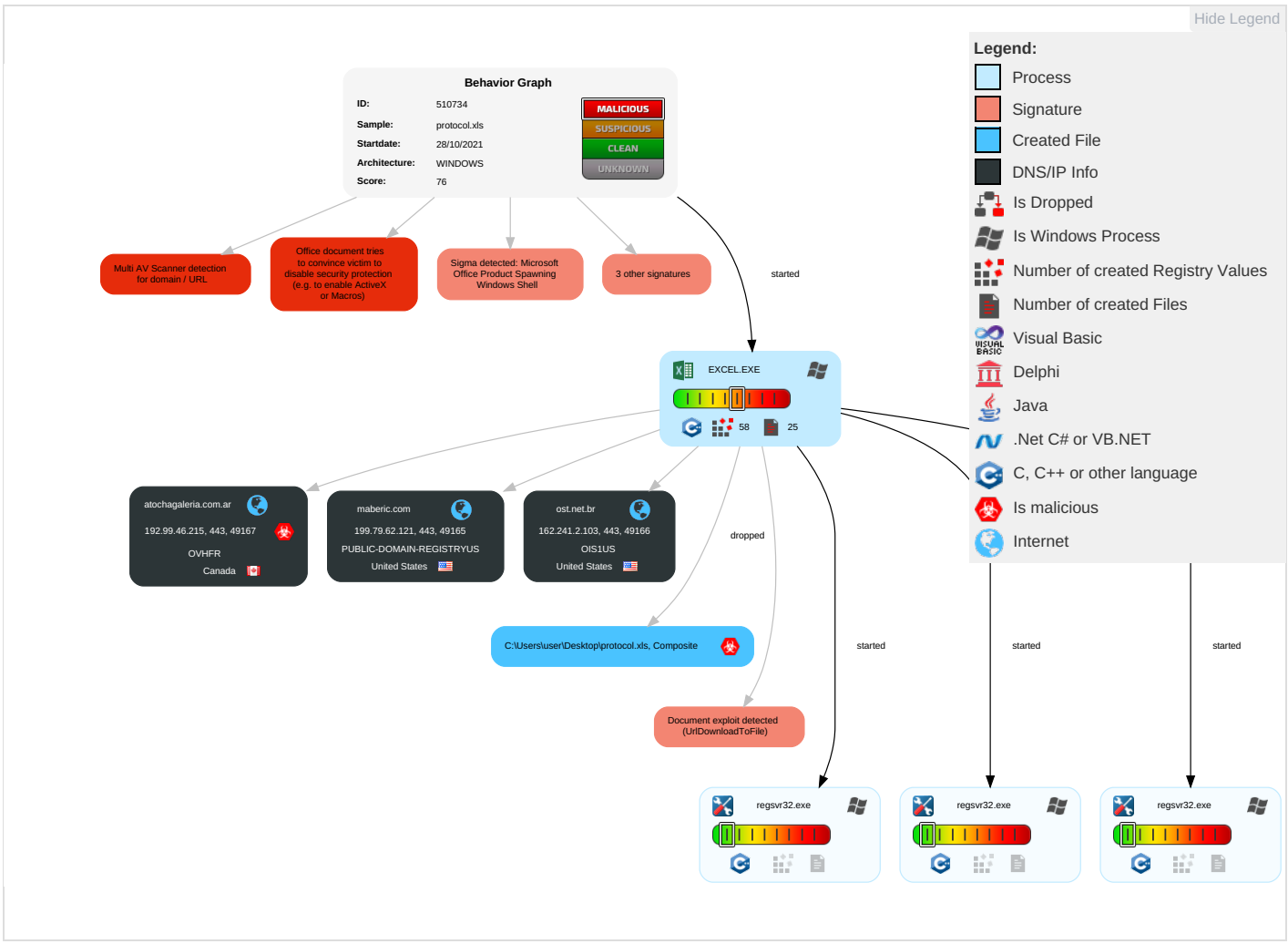
HIPS / PFW / Operating System Protection Evasion:

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	Re Se Ef
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Disable or Modify Tools 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap	

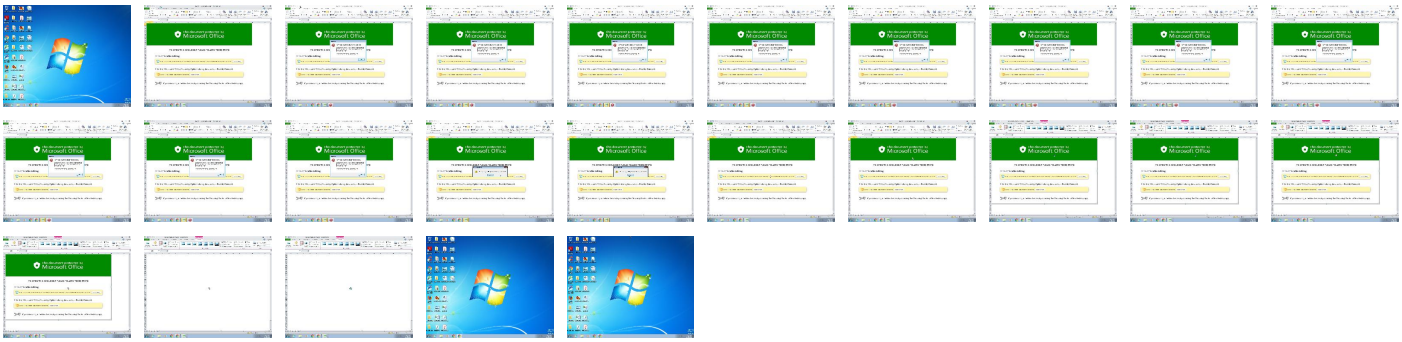
Behavior Graph

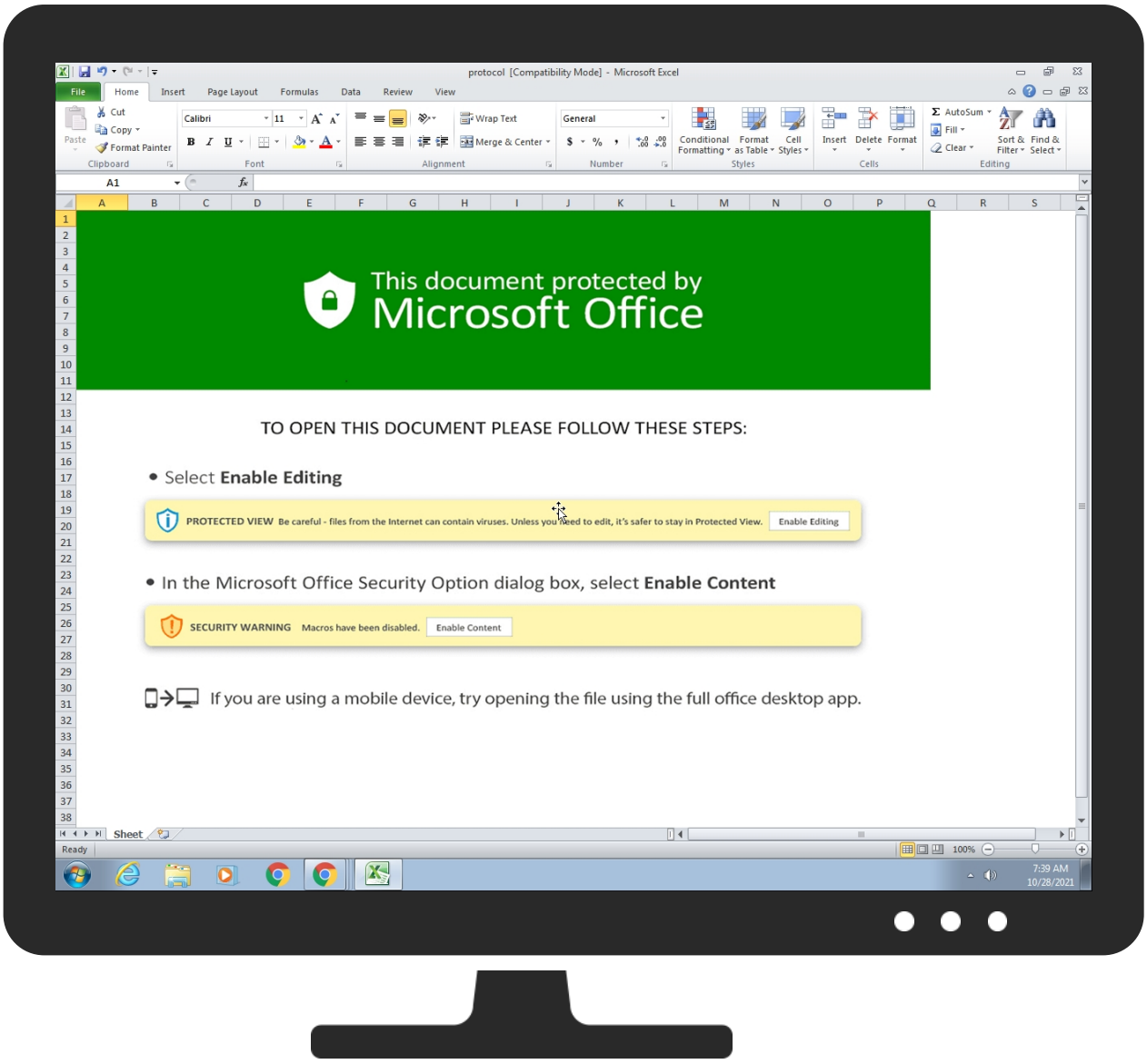


Screenshots

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
maberic.com	2%	Virustotal		Browse
atochagaleria.com.ar	5%	Virustotal		Browse
ost.net.br	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://atochagaleria.com.ar/CnijALAyxR/l.html	9%	Virustotal		Browse
http://https://atochagaleria.com.ar/CnijALAyxR/l.html	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	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	
http://https://maberic.com/3XRJdBEjFc/l.html	0%	Avira URL Cloud	safe	
http://https://ost.net.br/toXuNS00/l.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
maberic.com	199.79.62.121	true	false	• 2%, Virustotal, Browse	unknown
atochagaleria.com.ar	192.99.46.215	true	true	• 5%, Virustotal, Browse	unknown
ost.net.br	162.241.2.103	true	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://atochagaleria.com.ar/CnijALAyxR/l.html	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://maberic.com/3XRJdBEjFc/l.html	false	• Avira URL Cloud: safe	unknown
http://https://ost.net.br/toXuNS00/l.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.2.103	ost.net.br	United States		26337	OIS1US	false
199.79.62.121	maberic.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
192.99.46.215	atochagaleria.com.ar	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510734
Start date:	28.10.2021
Start time:	07:38:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	protocol.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.expl.winXLS@7/4@3/3
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 • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:38:21	API Interceptor	386x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.2.103	Order600567.exe	Get hash	malicious	Browse	• www.jogocertoptjc.com/dt9v/?9r=/6DROtFkY+DQN4u29C9TmrDbaQdWjbvTVyHiS8axtLai07FkaYsNfQsdClIJHXBP79fD&yt=WN9pTDLhcH
199.79.62.121	15Payment Notification Swift CopyX20 Confirmation.exe	Get hash	malicious	Browse	• alsaifpetrochem.com/zlokky/fre.php
192.99.46.215	5rNPlfqHxQ.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	WaPWtyR1ON.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	5rNPlfqHxQ.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	xBrGSNXGQ3.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	WaPWtyR1ON.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xBrGSNXGQ3.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	5fRfUQrSRk.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	8XpkPAA80t.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	5fRfUQrSRk.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	8XpkPAA80t.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	HBftgCs83Q.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	HBftgCs83Q.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	422RklrdvM.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	rLJ1CoEZEp.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	422RklrdvM.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	rLJ1CoEZEp.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	AJmEJMqAR9.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	fFnK0eybPw.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	AJmEJMqAR9.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/
	fFnK0eybPw.doc	Get hash	malicious	Browse	• benitezse guros.com. ar/dkywlkxs/Gd/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
maberic.com	protocol-1096018033.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1096018033.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1441399238.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1441399238.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1086855687.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1086855687.xls	Get hash	malicious	Browse	• 199.79.62.121
ost.net.br	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1441399238.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1441399238.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1086855687.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1086855687.xls	Get hash	malicious	Browse	• 162.241.2.103
atochagaleria.com.ar	protocol-1096018033.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1096018033.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1441399238.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1086855687.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1086855687.xls	Get hash	malicious	Browse	• 192.99.46.215

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OIS1US	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	protocol-1441399238.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1441399238.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1086855687.xls	Get hash	malicious	Browse	• 162.241.2.103
	protocol-1086855687.xls	Get hash	malicious	Browse	• 162.241.2.103
	POIM101385.exe	Get hash	malicious	Browse	• 192.185.147.203
	USD 58,508.80.exe	Get hash	malicious	Browse	• 192.185.147.203
	purchase order.exe	Get hash	malicious	Browse	• 192.185.147.203
	20211020 Copy of Customer transfer.exe	Get hash	malicious	Browse	• 192.185.147.203
	pGaL44AsT9.exe	Get hash	malicious	Browse	• 162.241.85.108
	ITFfhzMV0F.exe	Get hash	malicious	Browse	• 162.241.203.130
	dtMT5xGa54.exe	Get hash	malicious	Browse	• 162.241.85.108
	XWnSilQ3eG.exe	Get hash	malicious	Browse	• 192.185.147.20
	Payment.exe	Get hash	malicious	Browse	• 162.241.2.213
	INVOICE.exe	Get hash	malicious	Browse	• 162.241.2.213
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 162.241.85.65
	c0zG2sQGfpll1oV.exe	Get hash	malicious	Browse	• 162.241.2.213
	BxZ4Gj074H.exe	Get hash	malicious	Browse	• 192.185.147.20
	Payment.exe	Get hash	malicious	Browse	• 162.241.2.213
PUBLIC-DOMAIN-REGISTRYUS	Revised Purchase Order EU No.268766GMKD.exe	Get hash	malicious	Browse	• 208.91.198.143
	protocol-1096018033.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1096018033.xls	Get hash	malicious	Browse	• 199.79.62.121
	DHL Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment_Receipt_ 1791.xls	Get hash	malicious	Browse	• 162.215.252.35
	protocol-1441399238.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1441399238.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1086855687.xls	Get hash	malicious	Browse	• 199.79.62.121
	protocol-1086855687.xls	Get hash	malicious	Browse	• 199.79.62.121
	PO#098273.html	Get hash	malicious	Browse	• 208.91.199.181
	PO#098273.html	Get hash	malicious	Browse	• 208.91.199.181
	Sales_ReceiptX0480.xls	Get hash	malicious	Browse	• 199.79.63.90
	PaymentXAdviceX-RefXGLV403445242X.exe	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order 3920.exe	Get hash	malicious	Browse	• 208.91.198.143
	REVISED PURCHASE ORDER 26 PRECIOUSE STONE 65441QQMD.doc	Get hash	malicious	Browse	• 208.91.199.224
	tools-2123227448.xls	Get hash	malicious	Browse	• 162.215.253.110
	tools-2123227448.xls	Get hash	malicious	Browse	• 162.215.253.110
	RFQ_PI02102110.exe	Get hash	malicious	Browse	• 162.215.249.113
	REVISE INVOICE_09812300.exe	Get hash	malicious	Browse	• 111.118.215.189
	lCFjxhAqu3.exe	Get hash	malicious	Browse	• 208.91.199.64
OVHFR	dot#U007eremit-2458 xls.HtmL	Get hash	malicious	Browse	• 145.239.131.55
	SecuriteInfo.com.Drixed-FJXAE4472036314.31475.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXAE4472036314.31475.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJX22779BFC1D68.14546.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJX345EADC8B1F5.514.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Drixed-FJXE53A16BEA791.13728.dll	Get hash	malicious	Browse	• 149.202.179.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.dll	Get hash	malicious	Browse	• 149.202.17 9.100
	SecuriteInfo.com.Trojan.Win32.Save.a.28377.dll	Get hash	malicious	Browse	• 149.202.17 9.100
	SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.17 9.100
	SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.17 9.100
	protocol-1096018033.xls	Get hash	malicious	Browse	• 192.99.46.215
	protocol-1096018033.xls	Get hash	malicious	Browse	• 192.99.46.215
	arm7	Get hash	malicious	Browse	• 8.33.207.78
	#U0191ACTU#U0156A_wfpqacDkwlb__Z2676679.vbs	Get hash	malicious	Browse	• 144.217.33.249
	Byov62cXa1.exe	Get hash	malicious	Browse	• 94.23.24.82

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	UW_230 West 41st St_20211027.xlsm	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Sales_Receipt_ 5054.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Payment_Receipt_ 1791.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Early_Access.-3878_20211027.xlsb	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Casting Invite.-859403670_20211027.xlsb	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	protocol-1441399238.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	protocol-1086855687.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Purchase_Order 8328.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	payment.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Sales_ReceiptX0480.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	1.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	1.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	PI 210907-06.doc	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	D7yqLbdq4X.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	tools-2123227448.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	guide-2065442538.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	SMC Req Offer.doc	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Purchase Order-262021.doc	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	purchase order # 4459.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\CD1E.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaITlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF2671737F09DCABAC.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF9858F0CABAD63058.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.293601509610633
Encrypted:	false
SSDEEP:	768:RkG/Kpb8rGYrMPe3q7Q0XV5xtezEs/68/dgANZQ47c:R5Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dW
MD5:	8C23375CF5836B68FB406EFDF3D85D64
SHA1:	A47461CCABF50C3C897A8C28B38EFC41873792A6
SHA-256:	F9AB83436C0C8249AB22E8C793CBF6762CB2E543D9F2530AADD3BE64B91115BC
SHA-512:	5E49700C01CA5479C9ACE8ED4718336B76582B73364147F68A698E09579A3D315A646577FA1CDE1F07511B17A7B0CF98D64EAD597B4E05187BF925AABB656173
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF9858F0CABAD63058.TMP	
Preview:	.....

C:\Users\user\Desktop\protocol.xls	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Oct 27 10:45:18 2021, Security: 0
Category:	dropped
Size (bytes):	84992
Entropy (8bit):	6.331531840784684
Encrypted:	false
SSDEEP:	1536:85Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dgA91vrVmxJiME2GhdD52lZPFu1AOgo+tJ:qKpb8rGYrMPe3q7Q0XV5xtezEsi8/dg3
MD5:	FCBB9997C6F9C1E1CF03BB7554D83C4B
SHA1:	6E77EE067BC79ED701E1B5A47B5ACA4835DDEC6F
SHA-256:	68FAFB14CADA932D9A1C6907B09539764DFB0D598B108554EC6B7AF68F634819
SHA-512:	043E3C90D9A7291D9705D727F8D636FD100C71E4A4291499109E3843F4926FE1A1D7A96CCAD5A35AF2D711149636259CB7F1C33268B300B9C290BD66C70D5F8F
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\protocol.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\protocol.xls, Author: Joe Security
Reputation:	low
Preview:	.....>..... .....ZO..... .....\.p....user.8.=. B.....a.....=. .....=.....Ve18.....X.@..... ..."..... 1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Oct 27 10:45:18 2021, Security: 0
Entropy (8bit):	6.330898760473774
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	protocol.xls
File size:	84992
MD5:	93383a84bdf0f5ff68b3bb6e30bcd2bb
SHA1:	455bb88e45935daa21c2bf86e2b48da0d7627025
SHA256:	ca641647b3e2102c7b8f0075f46d1e52618f9b597d4e5ca338dcfec8f1210c59
SHA512:	97f48985f590843852b2a3e3cb4c1708d68ca1dec19e22c4a568d7dffc92a0cbb0b43ce473127f7017ed40e45583e7a80bd9d7da78d25af777edf00280c6782e
SSDEEP:	1536:c5Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dgA91vrVmxJiME2GhdD52lZPFu1AOgo+tO:KKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgl
File Content Preview:	.....>..... .....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "protocol.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2021-10-27 09:45:18
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 07:39:03.218375921 CEST	192.168.2.22	8.8.8.8	0x6519	Standard query (0)	maberic.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:39:04.231115103 CEST	192.168.2.22	8.8.8.8	0xe4ea	Standard query (0)	ost.net.br	A (IP address)	IN (0x0001)
Oct 28, 2021 07:39:06.598665953 CEST	192.168.2.22	8.8.8.8	0xa6bd	Standard query (0)	atochagaleria.com.ar	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 07:39:03.376092911 CEST	8.8.8.8	192.168.2.22	0x6519	No error (0)	maberic.com		199.79.62.121	A (IP address)	IN (0x0001)
Oct 28, 2021 07:39:04.408379078 CEST	8.8.8.8	192.168.2.22	0xe4ea	No error (0)	ost.net.br		162.241.2.103	A (IP address)	IN (0x0001)
Oct 28, 2021 07:39:06.618042946 CEST	8.8.8.8	192.168.2.22	0xa6bd	No error (0)	atochagaleria.com.ar		192.99.46.215	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- maberic.com
- ost.net.br
- atochagaleria.com.ar

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	199.79.62.121	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:39:03 UTC	0	OUT	GET /3XRJdBEjFc/l.html HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: maberic.com Connection: Keep-Alive
2021-10-28 05:39:04 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:39:04 GMT Server: nginx/1.19.5 Content-Type: text/html; charset=UTF-8 Content-Length: 0 X-Server-Cache: true X-Proxy-Cache: HIT Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	162.241.2.103	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:39:04 UTC	0	OUT	GET /toXuNS00/l.html HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: ost.net.br Connection: Keep-Alive
2021-10-28 05:39:06 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:39:04 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	192.99.46.215	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:39:06 UTC	1	OUT	GET /CnijALAyxR/l.html HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: atochagaleria.com.ar Connection: Keep-Alive
2021-10-28 05:39:07 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:39:11 GMT Server: Apache X-Powered-By: PHP/7.1.33 Cache-Control: max-age=2592000 Expires: Sat, 27 Nov 2021 05:39:11 GMT Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 196 Parent PID: 596

General

Start time:	07:38:14
Start date:	28/10/2021
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:	0x13f0a0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 2632 Parent PID: 196

General

Start time:	07:38:20
Start date:	28/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0xfff20000
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: 2792 Parent PID: 196

General

Start time:	07:38:21
Start date:	28/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0xfff20000
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: 2128 Parent PID: 196

General

Start time:	07:38:21
Start date:	28/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0xfff20000
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