ID: 510734
Sample Name: protocol.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 07:45:20
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

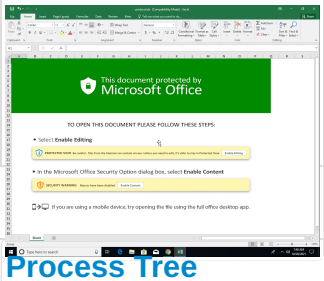
Windows Analysis Report protocol.xls

Overview

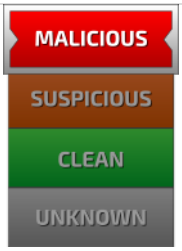
General Information

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

Most interesting Screenshot:



Detection



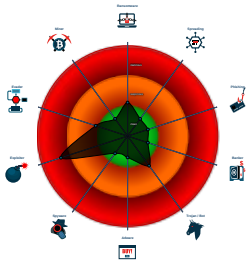
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Found detection on Joe Sandbox Clo…
- 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…
- Tries to load missing DLLs
- Uses a known web browser user age…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7044 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6616 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6588 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6656 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 426E7499F6A7346F0410DEAD0805586B)
- **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 0 0 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 0 0 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)

Found detection on Joe Sandbox Cloud Basic with higher score

HIPS / PFW / Operating System Protection Evasion:

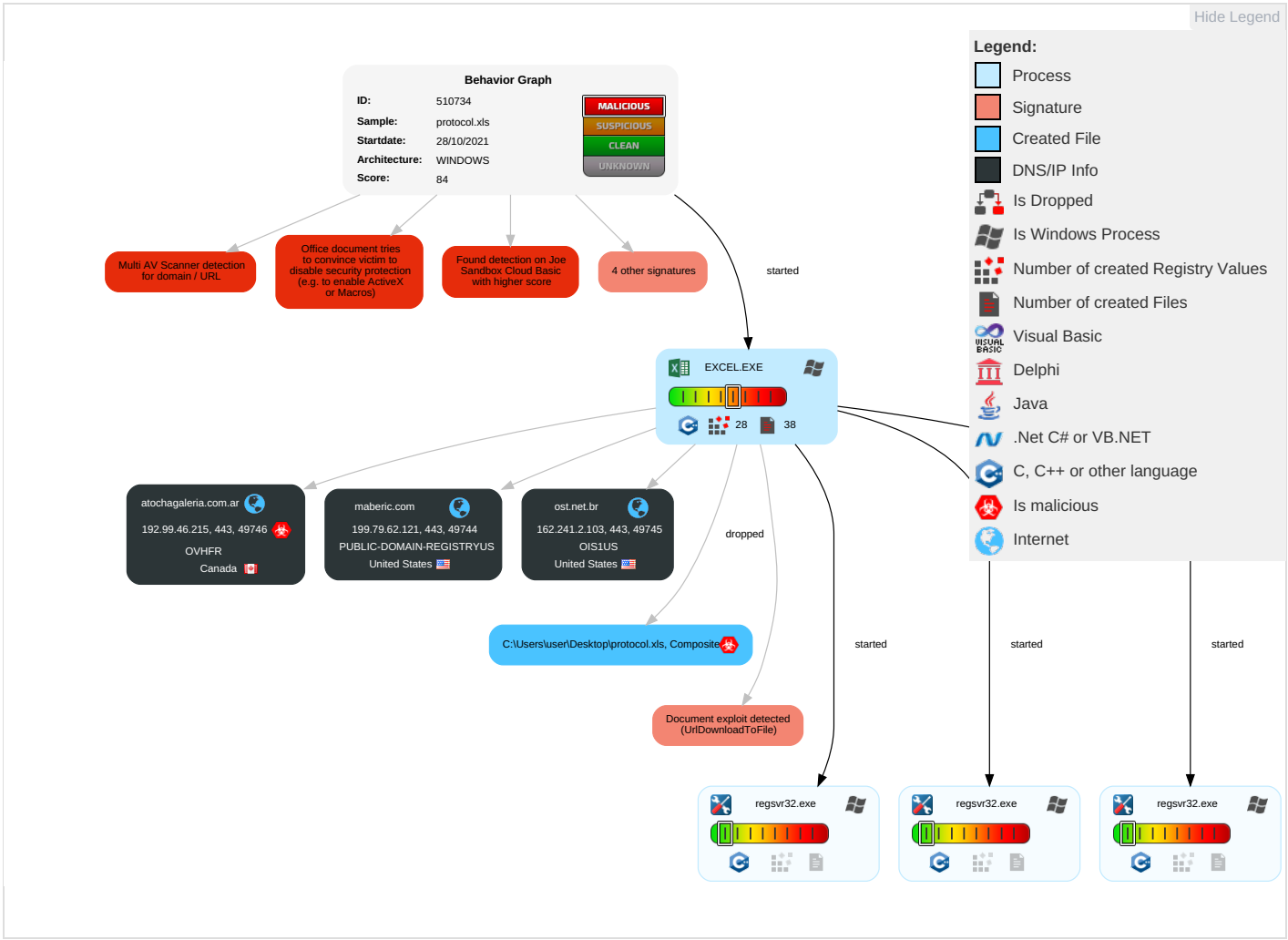
Yara detected hidden Macro 4.0 in Excel

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 1	DLL Side-Loading 1	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 1	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	DLL Side-Loading 1	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 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
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 1	SIM Card Swap		Ca Bi Fr

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

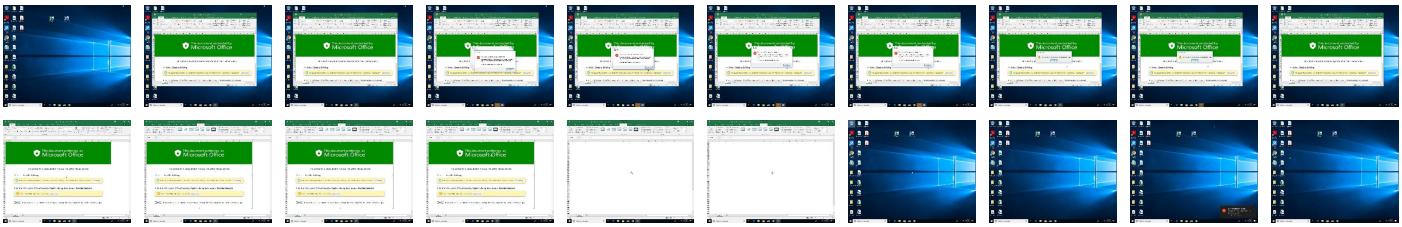
Behavior Graph

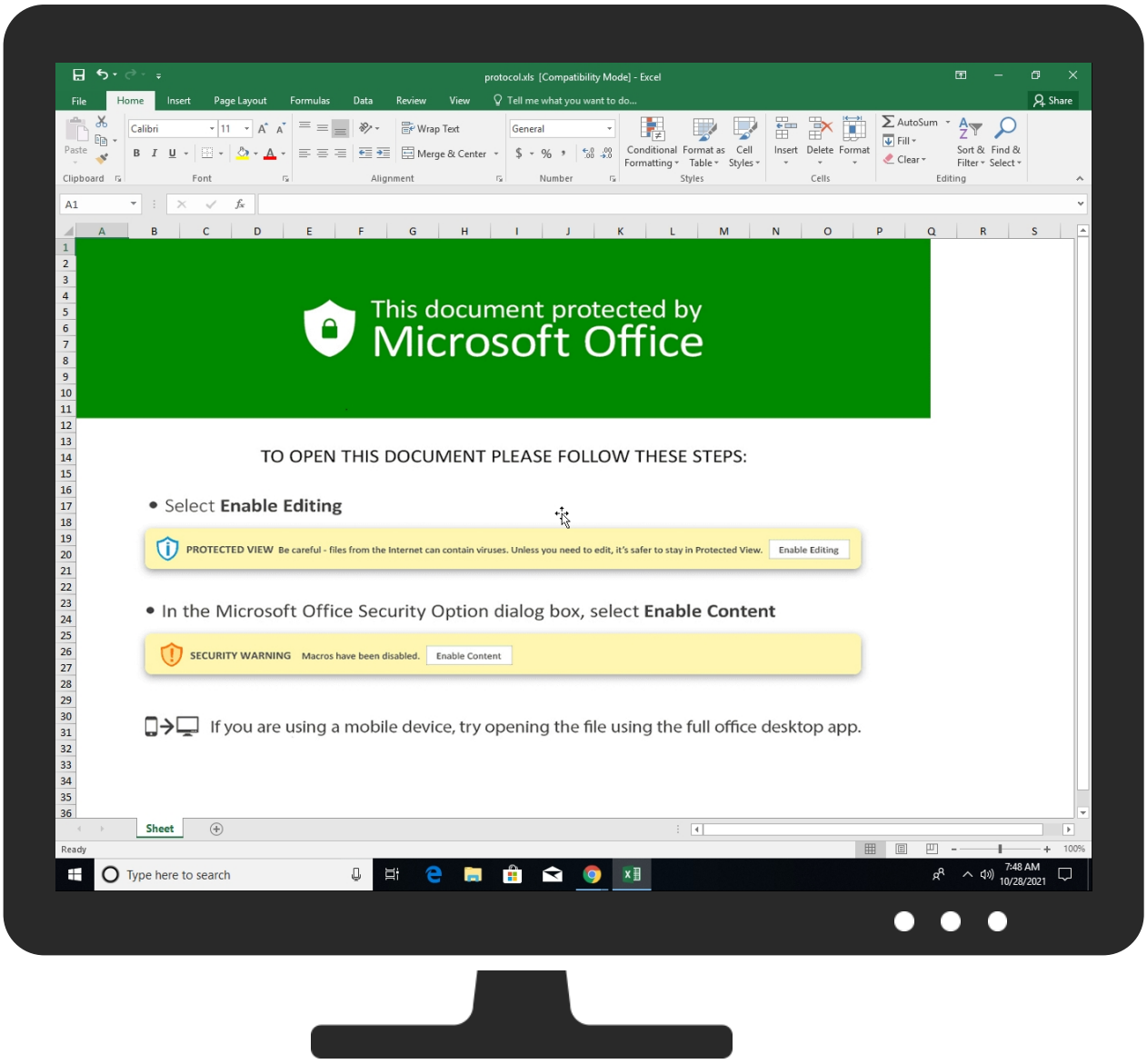


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

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://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://ost.net.br/toXuNS00/l.html	0%	Avira URL Cloud	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://atochagaleria.com.ar/CnijALAyxR/l.html	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://maberic.com/3XRJdBEjFc/l.html	0%	Avira URL Cloud	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	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://ost.net.br/toXuNS00/l.html	false	• Avira URL Cloud: safe	unknown
http://https://atochagaleria.com.ar/CnijALAyxR/l.html	true	• Avira URL Cloud: safe	unknown
http://https://maberic.com/3XRJdBEjFc/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:	07:45:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	protocol.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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:	mal84.expl.winXLS@7/5@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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

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/
	xBrGSNXGQ3.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	5fRfUQrSRk.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	8XpkPAA80t.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	5fRfUQrSRk.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	8XpkPAA80t.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	HBftgCs83Q.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	HBftgCs83Q.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	422RklrdvM.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	rLJ1CoEZEp.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	422RklrdvM.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	rLJ1CoEZEp.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	AJmEJMqAR9.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	fFnK0eybPw.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	AJmEJMqAR9.doc	Get hash	malicious	Browse	• benitezseguros.com.ar/dkywlkxs/Gd/
	fFnK0eybPw.doc	Get hash	malicious	Browse	• benitezseguros.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.xls	Get hash	malicious	Browse	• 162.241.2.103
	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.xls	Get hash	malicious	Browse	• 192.99.46.215
	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.xls	Get hash	malicious	Browse	• 162.241.2.103
	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
	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
PUBLIC-DOMAIN-REGISTRYUS	protocol.xls	Get hash	malicious	Browse	• 199.79.62.121
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
OVHFR	protocol.xls	Get hash	malicious	Browse	• 192.99.46.215
	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
	SecuriteInfo.com.Drixed-FJXEDADFD868F1D.21569.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.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.179.100
	SecuriteInfo.com.Trojan.Win32.Save.a.16213.dll	Get hash	malicious	Browse	• 149.202.179.100
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	TW_PURCHASE ORDER _BENTEX LTD_26201.exe	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	#Ud83d#Udd0a VM 9193404898.wav.html	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	dot#U007eremit-2458 xls.HtmL	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Chrome.Update.fb0369.js	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Chrome.Update.fb0369.js	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	protocol-1096018033.xls	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Invoice - INV-112289154.html	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	RYATPPETU.exe	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
	#U0191ACTU#U0156A_wfpqacDkwlb__Z2676679.vbs	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	3weZ3HvFxH.exe	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	89764583937678458745989.html	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	10272021-AM65Application.HTM	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
	Justificante de pago 876345864792456476253463474574535.vbs	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	Nwszeclpfkywlsrvlpglyrnsilmxebigcs.exe	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
	v2c.exe	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	sZFzUPz7Ee.exe	Get hash	malicious	Browse	• 162.241.2.103 • 199.79.62.121 • 192.99.46.215
	eMxXqjzvae.exe	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

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\ACCDA27E-452C-4E08-9584-F9C22DEC51A8	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	139130
Entropy (8bit):	5.358459697812044
Encrypted:	false
SSDEEP:	1536:gcQIfgxrBdA3gBwfnQ9DQW+zBY34Fi7nXboOidXVE6LWmE9:sWQ9DQW+zzXaH
MD5:	6000DCE79DF3716D19ECCDCC68705760
SHA1:	93522FF189A1580FEF5620A59213B337AC391B78
SHA-256:	05D31786D68307226F1891365E9513C803582679CDC5E7F8F21AEF169152B7FE
SHA-512:	25D98C15A82AE98C5747FBDEAD801EBCCD8883779CBDC8A143398E0BB0289767A32B768ADFD130B9E8D1694B10B7EB37AD9C5A9E3C425C239C6E014CDC15046
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-10-28T05:46:15">.. Build: 16.0.14618.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8C80DA27.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\8C80DA27.tmp	
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:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF5B4680BDC0A2AA0C.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.293912183277352
Encrypted:	false
SSDEEP:	768:bkG/Kpb8rGYrMPe3q7Q0XV5xtezEs/68/dgANZQ47c:b5Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dW
MD5:	8B0EF80202D4466B48973BFC38138879
SHA1:	19D588DFAAAF7CDB1571BE8F3BE365D6F4A47672
SHA-256:	D1ED8F8BD0320B84D50B1426797693A40EBC99916A08424223F1CE70FDBFAB0D
SHA-512:	9AD9280534BC0786A3D64B58EBC97553911872652E0150144B741DF6392C90EFB347543C290242262F4DA0158E7D008B47CFBC80022D1AFA6543BDC3CA365CB9
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF8E2EB8545C9796C0.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\Desktop\protocol.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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):	6.331473382025725
Encrypted:	false
SSDEEP:	1536:u5Kpb8rGYrMPe3q7Q0XV5xtezEsi8/dgA91vrVmxJiME2GhdD52lZPFu1AOgo+tn:gKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgJ
MD5:	5E4E5599073533B590D2581F768BFEB6
SHA1:	535B3C55198932C3AD4B0B9EF700C0FFC89F2C33
SHA-256:	F09A55BBA389F7EEBCB587C40C1F0ADF3BF8FE12FB3B7D6556A8163BFD946E21

C:\Users\user\Desktop\protocol.xls	
SHA-512:	F2B21D55806B27944BEB6D792D4C0C9AF389248D604504493E4EEDDD08FC6663CAAEF2586CA945D3509BC5677DD9B86FA7544EAB09B17603C4C164B2F0AC94C
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....pratesh.=. 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:	74ecd4c6c3c6c4d8

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 07:46:16.387759924 CEST	192.168.2.3	8.8.8.8	0x94c0	Standard query (0)	maberic.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:46:17.216913939 CEST	192.168.2.3	8.8.8.8	0x4c1e	Standard query (0)	ost.net.br	A (IP address)	IN (0x0001)
Oct 28, 2021 07:46:19.542339087 CEST	192.168.2.3	8.8.8.8	0x8d28	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
Oct 28, 2021 07:46:16.535312891 CEST	8.8.8.8	192.168.2.3	0x94c0	No error (0)	maberic.com		199.79.62.121	A (IP address)	IN (0x0001)
Oct 28, 2021 07:46:17.367312908 CEST	8.8.8.8	192.168.2.3	0x4c1e	No error (0)	ost.net.br		162.241.2.103	A (IP address)	IN (0x0001)
Oct 28, 2021 07:46:19.643416882 CEST	8.8.8.8	192.168.2.3	0x8d28	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	192.168.2.3	49744	199.79.62.121	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:46:16 UTC	0	OUT	GET /3XRJdBEjFc/l.html HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: maberic.com Connection: Keep-Alive
2021-10-28 05:46:17 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:46:17 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	192.168.2.3	49745	162.241.2.103	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:46:17 UTC	0	OUT	GET /toXuNS00/l.html HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: ost.net.br Connection: Keep-Alive
2021-10-28 05:46:19 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:46:17 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	192.168.2.3	49746	192.99.46.215	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-28 05:46:19 UTC	0	OUT	GET /CnijALAyxR/l.html HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: atochagaleria.com.ar Connection: Keep-Alive
2021-10-28 05:46:20 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 28 Oct 2021 05:46:24 GMT Server: Apache X-Powered-By: PHP/7.1.33 Cache-Control: max-age=2592000 Expires: Sat, 27 Nov 2021 05:46:24 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: 7044 Parent PID: 744

General

Start time:	07:47:02
Start date:	28/10/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xdf0000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6616 Parent PID: 7044

General

Start time:	07:47:09
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0xba0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 6588 Parent PID: 7044

General

Start time:	07:47:10
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0xba0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 6656 Parent PID: 7044

General

Start time:	07:47:10
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0xba0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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