ID: 532933
Sample Name: ClaimCopy-355714047-12022021.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:58:09
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

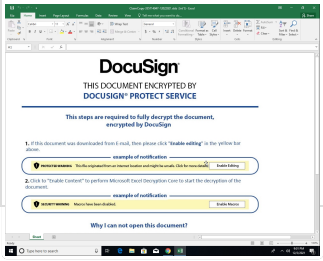
Windows Analysis Report ClaimCopy-355714047-12022…

Overview

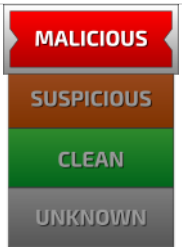
General Information

Sample Name:	ClaimCopy-355714047-12022021.xlsb
Analysis ID:	532933
MD5:	1f51fa867f5bbce…
SHA1:	2c690539b53f4db.
SHA256:	f3dc3443c7ba185..
Infos:	

Most interesting Screenshot:



Detection



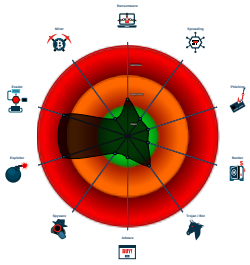
Hidden Macro 4.0

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: 5140 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 2484 cmdline: regsvr32 C:\ProgramData\Volet1.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4028 cmdline: regsvr32 C:\ProgramData\Volet2.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4248 cmdline: regsvr32 C:\ProgramData\Volet3.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 3324 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet4.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5320 cmdline: regsvr32 -e -n -i:&Tiposa!G22& C:\ProgramData\Volet5.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6200 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)

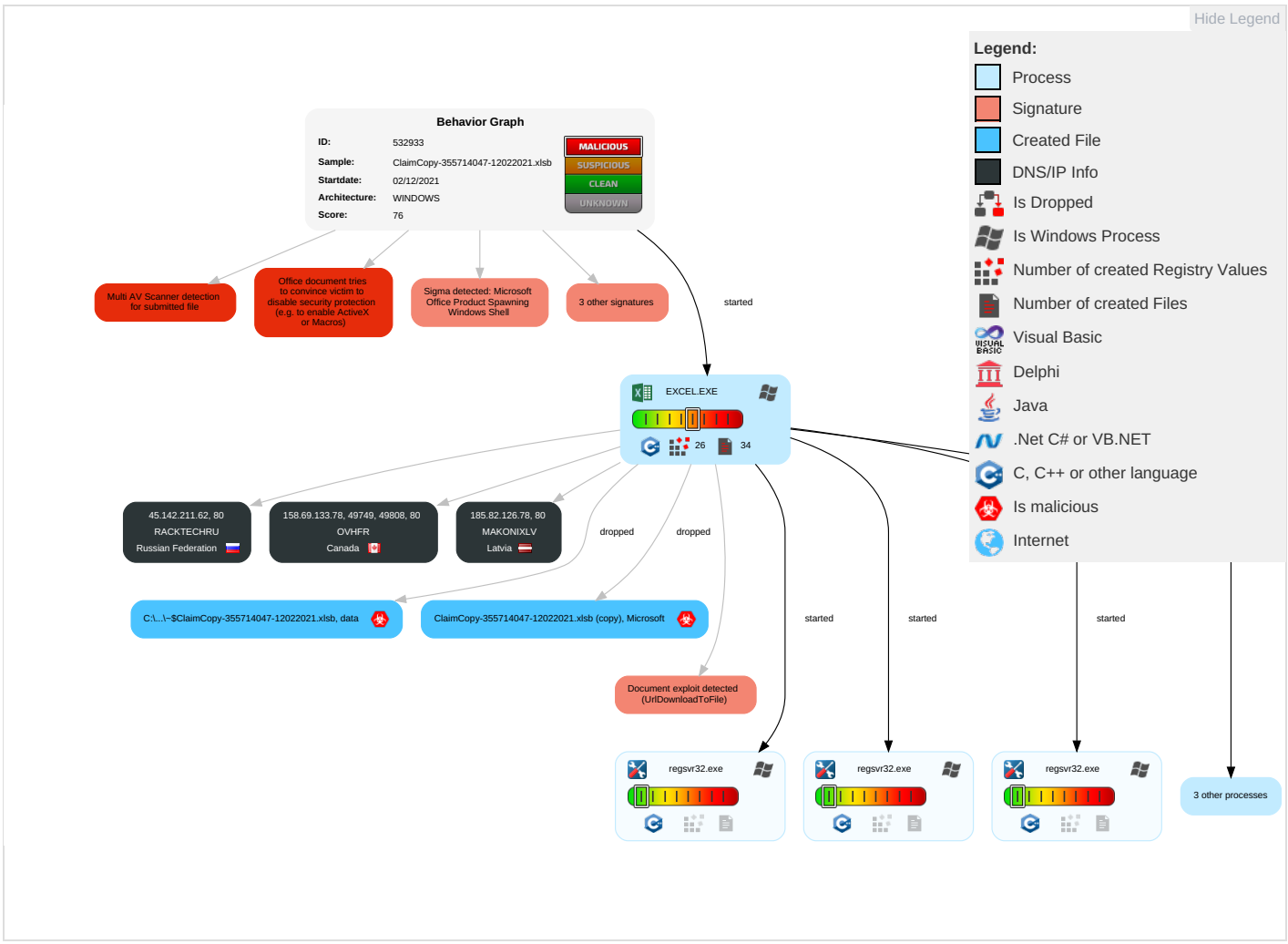
Found Excel 4.0 Macro with suspicious formulas

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

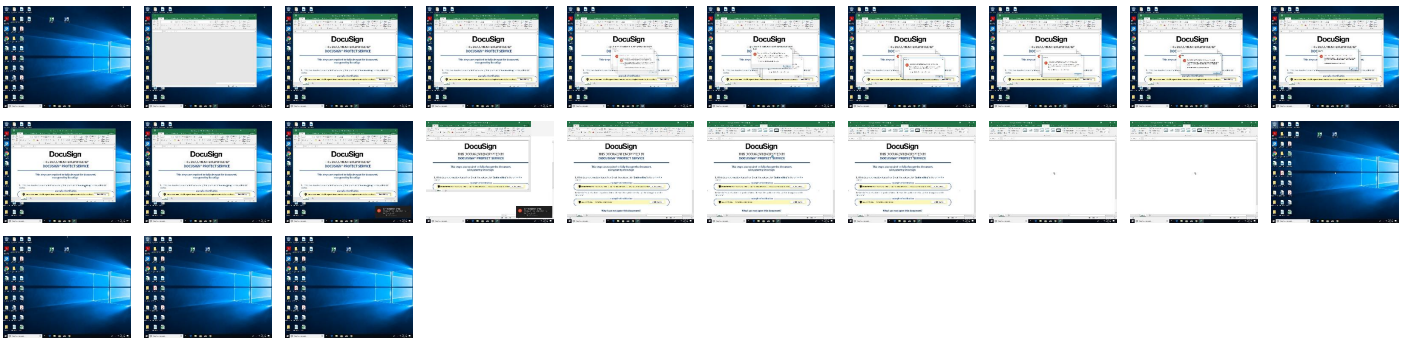
Behavior Graph

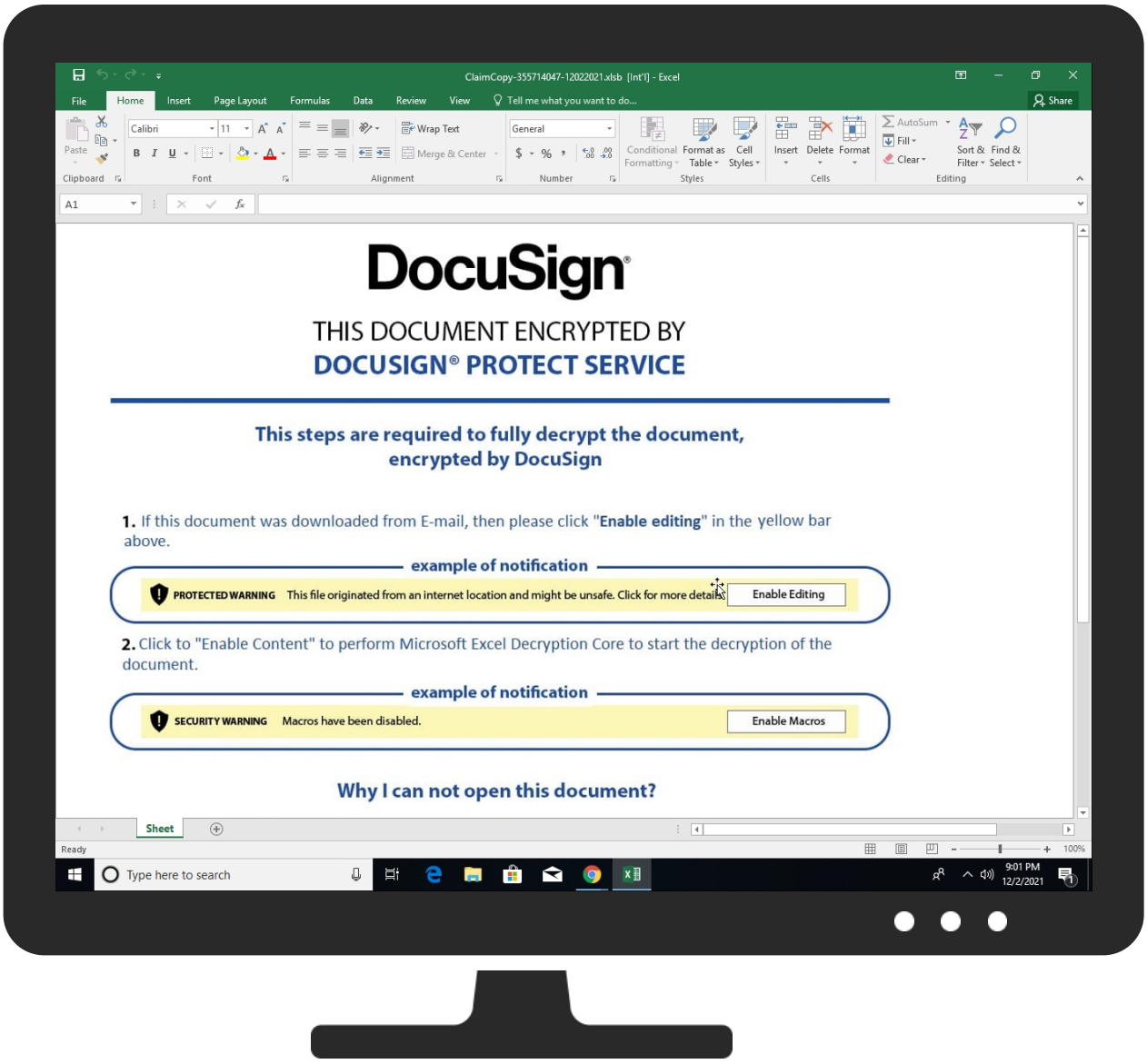


Screenshots

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-355714047-12022021.xlsb	10%	Virustotal		Browse

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://cortana.ai/apihttps://login.windows.net/common/oauth2/authorize	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	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.aadrm.comh	0%	Avira URL Cloud	safe	
http://https://api.cortana.ait	0%	Avira URL Cloud	safe	
http://45.142.211.62/823634401007.dat2vdom	0%	Avira URL Cloud	safe	
http://185.82.126.78/823634401007.datr	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFileBearer	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://outlook.office.com2;	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	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.comy	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comMBI	0%	Avira URL Cloud	safe	
http://https://substrate.office.comc	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://augloop.office.comLinkRequestApiPageTitleRetrievalhttps://uci.	0%	Avira URL Cloud	safe	
http://https://management.azure.comw	0%	Avira URL Cloud	safe	
http://https://settings.outlook.com&	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	URL Reputation	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://substrate.office.com$;	0%	Avira URL Cloud	safe	
http://45.142.211.62/823634401007.dat2	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://onedrive.live.comed	0%	Avira URL Cloud	safe	
http://https://webshell.suite.office.comu	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

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:	532933
Start date:	02.12.2021
Start time:	20:58:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 54s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	ClaimCopy-355714047-12022021.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:	32
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-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62/33759 1964609.dat2
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62/71020 3175032.dat2
	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-355714047-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/57476 6024224.dat2
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/33759 1964609.dat2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/71020/3175032.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/48062/8690611.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/93960/2286691.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78/53379/2932717.dat2
185.82.126.78	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78/33759/1964609.dat2
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78/71020/3175032.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78/48062/8690611.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78/93960/2286691.dat2
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78/53379/2932717.dat2

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RACKTECHRU	ClaimCopy-355714047-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 45.142.211.62
	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
	VKtClrdZz3.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
MAKONIXLV	ClaimCopy-355714047-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 185.82.126.78
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
OVHFR	ClaimCopy-355714047-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	7009.xlsx	Get hash	malicious	Browse	• 87.98.234.164
	TNT Documents.exe	Get hash	malicious	Browse	• 51.255.30.106
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	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	• 213.251.15 8.218
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 149.56.106.83
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 149.56.106.83
	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

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\1C879995-8362-47D0-A5BB-F2EF376F1B92	
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):	140402
Entropy (8bit):	5.356837185034186
Encrypted:	false
SSDEEP:	1536:NcQIfgxrBdA3gBwtnQ9DQW+zUk4Ff7nXmvid1XiE6LWmE9:XuQ9DQW+ziXfH
MD5:	F6274765DA606FDEF0078893DB63323A
SHA1:	5C236960557C236002232615189B2985479B5F87
SHA-256:	32A22CB3E4D579CD7B1FAA6DE03928CFA0829CC930EA9D88E13FC7F1E47B1F0F
SHA-512:	210AE0354205E6F5AE3B0562216194F52F1496C508E3B689F5DFB46DA87EE80FCB6C1C91F963D73A73415AA4847EEE8EA4AA5D87513939081703CDD7C0AEEBFB
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="2021-12-02T19:59:01">.. Build: 16.0.14729.30527-->.. <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\68B0554C.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\68B0554C.jpg	
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\0E340000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99472
Entropy (8bit):	7.830475726763584
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsU/B:Inc6EehCfCZpUHKGXbBKsii6
MD5:	E9F891518AF09FB0781A39B41EB33381
SHA1:	8E0D92F2700BF44B6BD6411FB89FF94565CDF0EE
SHA-256:	74CD0B58137FBAA2AB29D851602E0A86AB17372F5CB81EE753C9798C24F48B15
SHA-512:	44817AEFB8FFD5D6E54853B9BF0EA118AA8B4503A0BB46E22E9C95FE389FC20AE0354E7C1621A39C1FFE56474B4511F5EE3FD86678BE2B1547B1711103BC6B2E
Malicious:	false
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\0E340000: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
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\ClaimCopy-355714047-12022021.xlsb (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	99472
Entropy (8bit):	7.830475726763584
Encrypted:	false
SSDEEP:	1536:IhyB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsU/B:Inc6EehCfCZpUHKGXbBKsii6
MD5:	E9F891518AF09FB0781A39B41EB33381
SHA1:	8E0D92F2700BF44B6BD6411FB89FF94565CDF0EE
SHA-256:	74CD0B58137FBAA2AB29D851602E0A86AB17372F5CB81EE753C9798C24F48B15

C:\Users\user\Desktop\ClaimCopy-355714047-12022021.xlsb (copy)	
SHA-512:	44817AEFB8FFD5D6E54853B9BF0EA118AA8B4503A0BB46E22E9C95FE389FC20AE0354E7C1621A39C1FFE56474B4511F5EE3FD86678BE2B1547B1711103BC6B2E
Malicious:	**true**
Preview:	PK.....!.V.....[Content_Types].xml ...(..... ....U.n.0.}G..".....BM..C.....^|.x8.....v...&kTx.....{..e....jg+...V.....{V`.VI.,TI....._.n... ...1..B`.B'.;...I\.d.ah...O..X,....6.1q....I..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\~$ClaimCopy-355714047-12022021.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:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.831014482033694
TrID:	• Microsoft Excel Office Binary workbook document (40504/1) 83.51% • ZIP compressed archive (8000/1) 16.49%
File name:	ClaimCopy-355714047-12022021.xlsb
File size:	99677
MD5:	1f51fa867f5bbce3ab1cc40bf75f7f9b
SHA1:	2c690539b53f4db35af92e2b88880c3d76fcd323
SHA256:	f3dc3443c7ba185b1c8eff63807384e9bb6734fa0774d9964213dd9baf3fb3c3
SHA512:	cf98c415cee36aa57815e5f0b2a0708ca7035ec34c46848cc47fb07859d013f5f9c5651d32478a2fe4ef62730cf450570d28ae18ec884a8a0612e739a37e8f84
SSDEEP:	1536:rMB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUfp:/c6EehCfCZpUHKGXbBKsiiOp
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-355714047-12022021.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
12/02/21-20:49:37.323864	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	158.69.133.78	192.168.2.22
12/02/21-20:51:44.215042	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49175	158.69.133.78	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 158.69.133.78

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	158.69.133.78	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:59:27.512147903 CET	1372	OUT	GET /823634401007.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 20:59:28.168723106 CET	1373	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 19:59:28 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	49808	158.69.133.78	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 21:00:31.582458973 CET	6428	OUT	GET /823634401007.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 21:00:32.071048975 CET	6429	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 20:00:32 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: 5140 Parent PID: 744

General

Start time:	20:58:59
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:	0x810000
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: 2484 Parent PID: 5140

General

Start time:	21:00:32
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet1.ocx
Imagebase:	0xe80000
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: 4028 Parent PID: 5140

General

Start time:	21:00:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet2.ocx
Imagebase:	0xe80000
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: 4248 Parent PID: 5140

General

Start time:	21:00:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 C:\ProgramData\Volet3.ocx
Imagebase:	0xe80000
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: 3324 Parent PID: 5140

General

Start time:	21:00:34
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:	0xe80000
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: 5320 Parent PID: 5140

General

Start time:	21:00:34
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:	0xe80000
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: 6200 Parent PID: 5140

General

Start time:	21:00:35
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:	0xe80000
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