ID: 532936
Sample Name: ComplaintDetails-1244065104-Nov-17.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:54:03
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

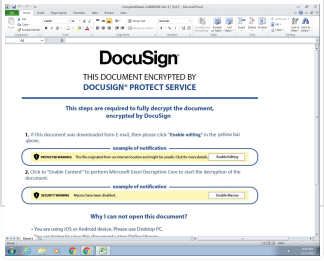
Windows Analysis Report ComplaintDetails-1244065104…

Overview

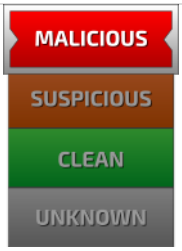
General Information

Sample Name:	ComplaintDetails-1244065104-Nov-17.xlsb
Analysis ID:	532936
MD5:	cfee2afbf9c7456…
SHA1:	2d43d6ad54fb33c.
SHA256:	0a7656fab771936.
Infos:	

Most interesting Screenshot:



Detection



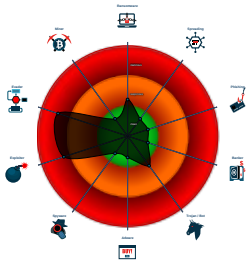
Hidden Macro 4.0

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2844 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 508 cmdline: regsvr32.exe ..\Tot1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2956 cmdline: regsvr32.exe ..\Tot2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2568 cmdline: regsvr32.exe ..\Tot3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found malicious Excel 4.0 Macro

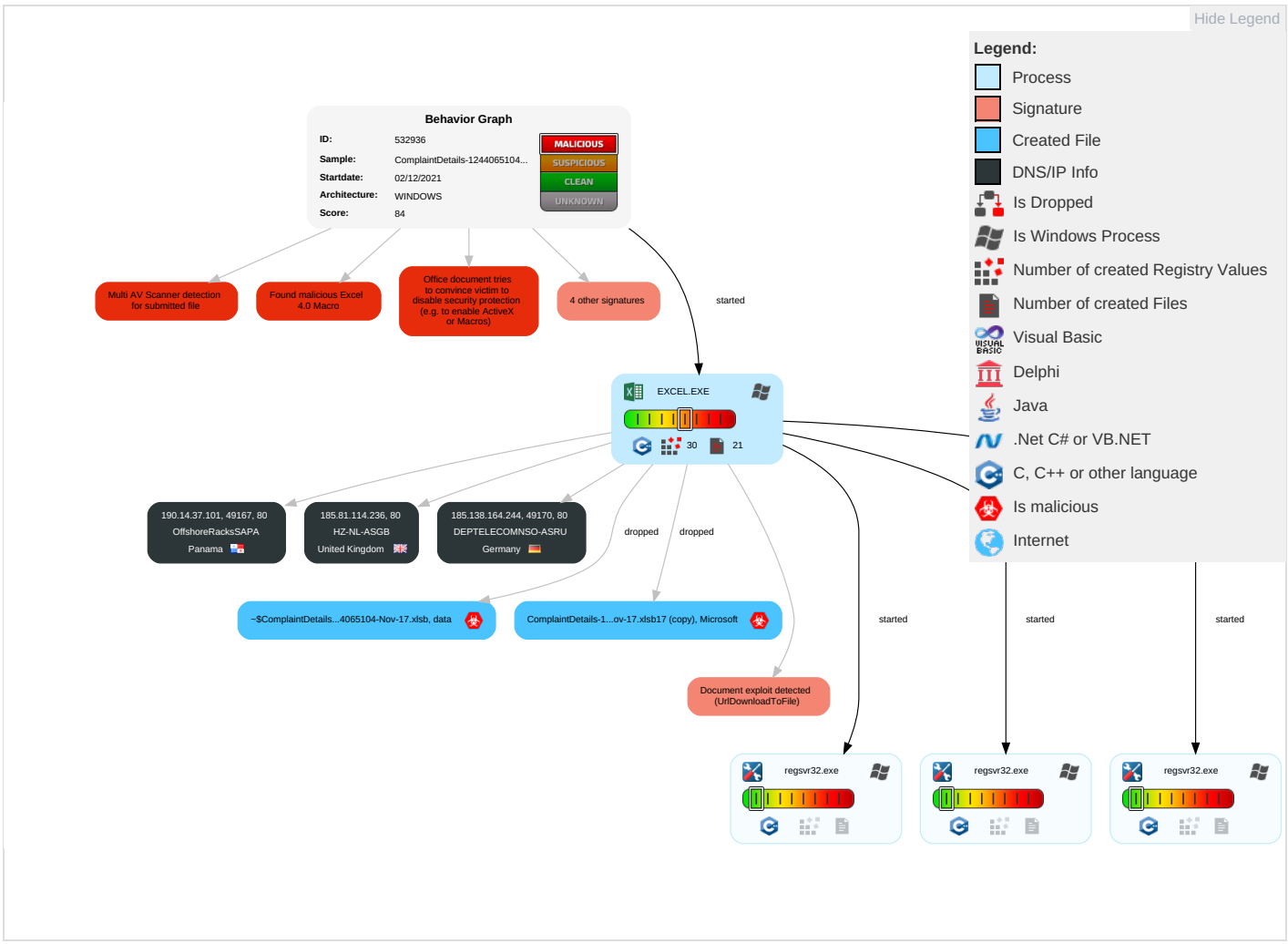
Found Excel 4.0 Macro with suspicious formulas

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
Valid Accounts	Scripting 3	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 4	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

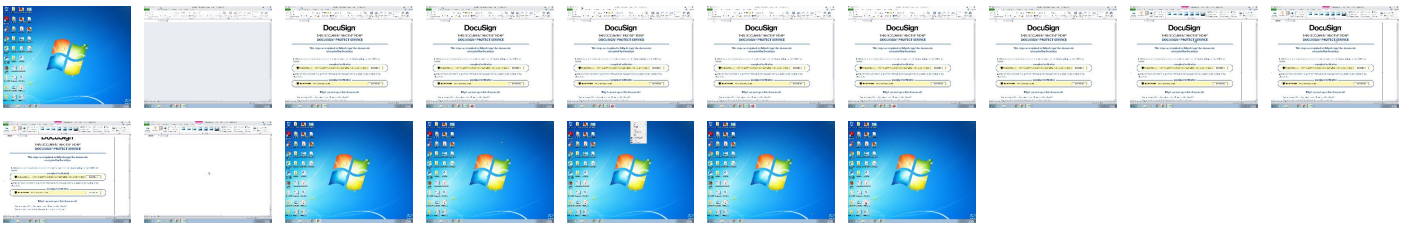
Behavior Graph

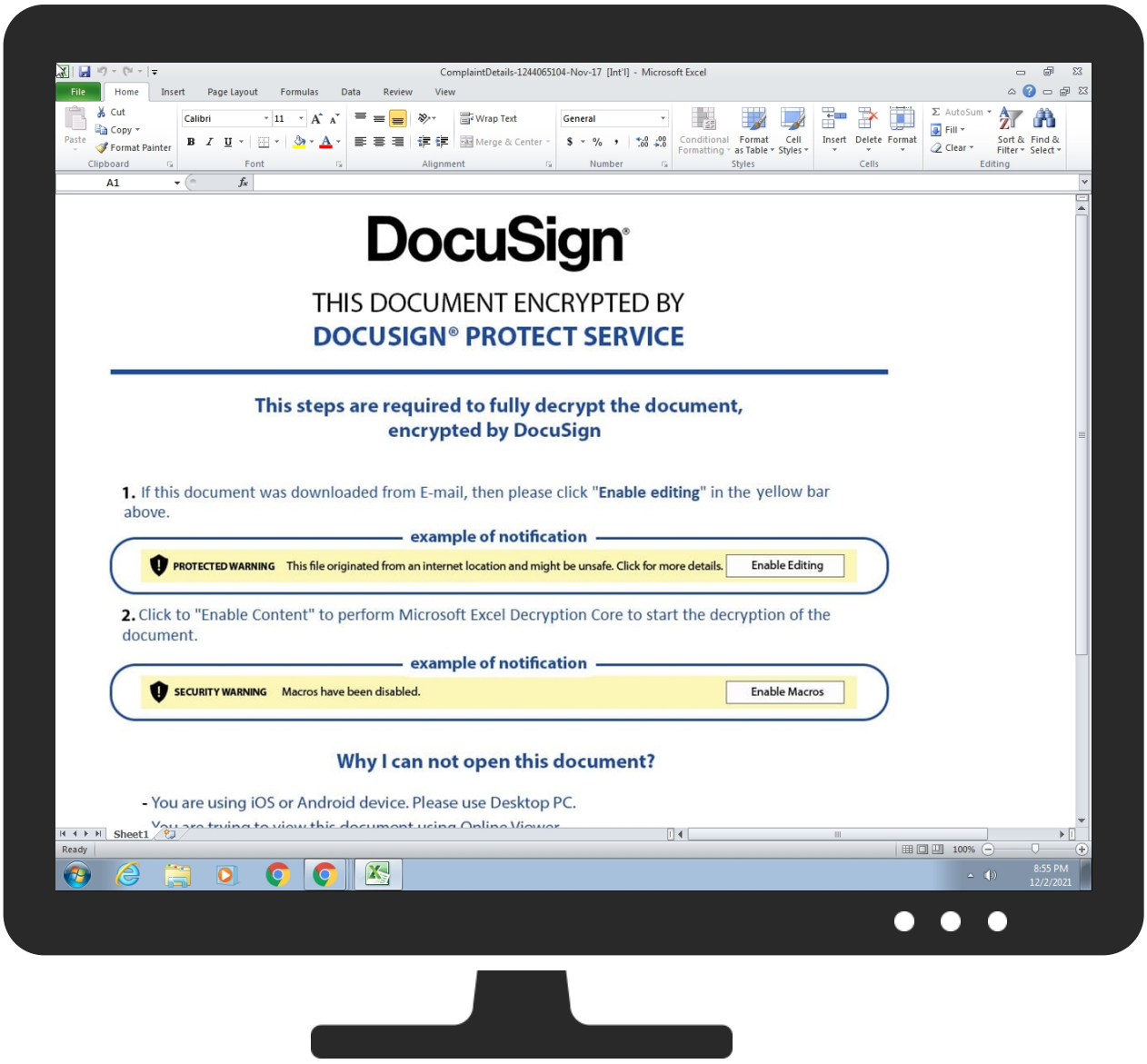


Screenshots

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
ComplaintDetails-1244065104-Nov-17.xlsb	6%	Metadefender		Browse
ComplaintDetails-1244065104-Nov-17.xlsb	39%	ReversingLabs	Document-Office.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.138.164.244/44532.8710387731.date9:00	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://185.138.164.244/E	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	
http://190.14.37.101/A	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://190.14.37.101/44532.8710387731.dat	0%	Avira URL Cloud	safe	
http://185.138.164.244/44532.8710387731.datc9:00	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://185.81.114.236/C	0%	Avira URL Cloud	safe	
http://185.138.164.244/44532.8710387731.dat	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://190.14.37.101/44532.8710387731.dat	false	• Avira URL Cloud: safe	unknown
http://185.138.164.244/44532.8710387731.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
190.14.37.101	unknown	Panama		52469	OffshoreRacksSAPA	false
185.138.164.244	unknown	Germany		50451	DEPTELECOMNSO-ASRU	false
185.81.114.236	unknown	United Kingdom		59711	HZ-NL-ASGB	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532936
Start date:	02.12.2021
Start time:	20:54:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ComplaintDetails-1244065104-Nov-17.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.expl.evad.winXLSB@7/5@0/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:55:10	API Interceptor	3x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEPTELECOMNSO-ASRU	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 185.138.164.46
	10KaQvX7O7.exe	Get hash	malicious	Browse	• 185.138.164.150
	mG5GGD3Pm6.exe	Get hash	malicious	Browse	• 185.138.164.150
	___ __ 9_.exe	Get hash	malicious	Browse	• 185.138.164.150
	mAISpSSZ7f.exe	Get hash	malicious	Browse	• 185.138.164.150
	eLZzxG56uH.exe	Get hash	malicious	Browse	• 185.138.164.150
	SKM_C258.EXE	Get hash	malicious	Browse	• 185.138.164.150
	CPHB7Z2buG.exe	Get hash	malicious	Browse	• 185.138.164.150
	aylGgMNibQ.exe	Get hash	malicious	Browse	• 185.138.164.150

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	V3fm0d84mp.exe	Get hash	malicious	Browse	• 185.138.164.150
	Aqlmlmmeey.exe	Get hash	malicious	Browse	• 185.138.164.150
	6lGJNtdKHt.exe	Get hash	malicious	Browse	• 185.138.164.150
	nGiDZ9ZC2d.exe	Get hash	malicious	Browse	• 185.138.164.150
	xx2wsaL3cJ.exe	Get hash	malicious	Browse	• 185.138.164.150
	75fcGkVO1k.exe	Get hash	malicious	Browse	• 185.138.164.150
	8aAG42oljb.exe	Get hash	malicious	Browse	• 185.138.164.150
	Zq0u07ZGkg.exe	Get hash	malicious	Browse	• 185.138.164.150
	jUV82t8dgh.exe	Get hash	malicious	Browse	• 185.138.164.150
	SecuriteInfo.com.W32.AIDetect.malware1.14529.exe	Get hash	malicious	Browse	• 185.138.164.150
	art185.exe	Get hash	malicious	Browse	• 185.138.164.157
OffshoreRacksSAPA	ContractCopy-2007317195-Nov-18.xlsb	Get hash	malicious	Browse	• 190.14.37.186
	ContractCopy-2007317195-Nov-18.xlsb	Get hash	malicious	Browse	• 190.14.37.186
	Srv-Interrupt-95268364-Nov-10.xlsm	Get hash	malicious	Browse	• 190.14.37.9
	Srv-Interrupt-95268364-Nov-10.xlsm	Get hash	malicious	Browse	• 190.14.37.9
	rzdYBz3qEl.xlsb	Get hash	malicious	Browse	• 190.14.37.186
	PRSM 15433.xlsb	Get hash	malicious	Browse	• 190.14.37.182
	PRSM 15433.xlsb	Get hash	malicious	Browse	• 190.14.37.182
	CLMCP 9215 Nov 15 (374).xlsb	Get hash	malicious	Browse	• 190.14.37.84
	CLMCP 9215 Nov 15 (374).xlsb	Get hash	malicious	Browse	• 190.14.37.84
	CLMCP 9215 Nov 15 (383).xlsb	Get hash	malicious	Browse	• 190.14.37.84
	CLMCP 9215 Nov 15 (383).xlsb	Get hash	malicious	Browse	• 190.14.37.84
	11008767374-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	11008767374-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	1359055027-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	1359055027-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	1359055027-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	11625955776-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	Compl-598085012-Nov-08.xlsm	Get hash	malicious	Browse	• 190.14.37.28
	1589557877-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89
	1589557877-11112021.xlsm	Get hash	malicious	Browse	• 190.14.37.89

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DC095B18.jpg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1098x988, frames 3
Category:	dropped
Size (bytes):	85681
Entropy (8bit):	7.915850776614707
Encrypted:	false
SSDEEP:	1536:wB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUw:Pc6EehCfCZpUHKGXbBKsiit
MD5:	4F100E2CEFED046B44EC799015B454EF
SHA1:	5149E5D1B5212C77B3548914E9B47D67B4BEA574
SHA-256:	D30B441AB0E88A1487F29A80D63E2A4865A3F5DF7854FB8359B354397F807E2C
SHA-512:	153581151434815CC17E88D587FF6A6AF8F7154B4A05146453A9814F662C68D79F1063BDD9F789A1DB2F5818D199EF600703F8BC35785B0705332EC231F35A14

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DC095B18.jpg	
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\ComplaintDetails-1244065104-Nov-17.xlsb17 (copy)	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	97082
Entropy (8bit):	7.8327461553726785
Encrypted:	false
SSDEEP:	1536:CGB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUt6A:CBc6EehCfCZpUHKGXbBKsiiM6A
MD5:	DDAD6F2ECE4007B9ED5F4AE21F009B8D
SHA1:	AFEFC9E3AA046422A0B395D7E63738B245DBB9F3
SHA-256:	0201B654E9DCFCAB3D21F3B15705041B214FCEC3296821522578F671C88959B8
SHA-512:	A5AD9B2F7F97CD9E103514E5EEA4A1CA99976E0919F9E8ABC96B83E3F04C1532705FC334EA7F6145DA402EBFC06D8E9D3BF07CD4429ACBE66E2D000D855200A1
Malicious:	**true**
Reputation:	low
Preview:	PK.....!..E.....~.....[Content_Types].xml ...(..... ....U.n.0....?..."......C..=.....q-1.H..I..v.V.....z..g8Z.....!....K....6..F...R.....F...;@q.~.fu.....=6.'.....A...<?.4h....._..u.X.Wm...j..b.....J....{Y..:Fg [M.P.....m.Nb.@..:.....s..hfQG..8|A.....ddY..6.;.9...L;....n..CN.>B..~.n%k.....Q[.....*...e.e.6.cF.e9Sj..Wo`;K.q.....5^...w...O.T9...n.v...6.....,4O.(.....G....u.sC...<...'.L.3.:.. >....YEvD.n.....i....@.....T ...)D.y.`~g..VF.. ...u.

C:\Users\user\Desktop\D1440000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	97082
Entropy (8bit):	7.8327461553726785
Encrypted:	false
SSDEEP:	1536:CGB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUt6A:CBc6EehCfCZpUHKGXbBKsiiM6A
MD5:	DDAD6F2ECE4007B9ED5F4AE21F009B8D
SHA1:	AFEFC9E3AA046422A0B395D7E63738B245DBB9F3
SHA-256:	0201B654E9DCFCAB3D21F3B15705041B214FCEC3296821522578F671C88959B8
SHA-512:	A5AD9B2F7F97CD9E103514E5EEA4A1CA99976E0919F9E8ABC96B83E3F04C1532705FC334EA7F6145DA402EBFC06D8E9D3BF07CD4429ACBE66E2D000D855200A1
Malicious:	false
Reputation:	low
Preview:	PK.....!..E.....~.....[Content_Types].xml ...(..... ....U.n.0....?..."......C..=.....q-1.H..I..v.V.....z..g8Z.....!....K....6..F...R.....F...;@q.~.fu.....=6.'.....A...<?.4h....._..u.X.Wm...j..b.....J....{Y..:Fg [M.P.....m.Nb.@..:.....s..hfQG..8|A.....ddY..6.;.9...L;....n..CN.>B..~.n%k.....Q[.....*...e.e.6.cF.e9Sj..Wo`;K.q.....5^...w...O.T9...n.v...6.....,4O.(.....G....u.sC...<...'.L.3.:.. >....YEvD.n.....i....@.....T ...)D.y.`~g..VF.. ...u.

C:\Users\user\Desktop\D1440000:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\~$ComplaintDetails-1244065104-Nov-17.xlsb	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.8328127669623
TrID:	• Microsoft Excel Office Binary workbook document (40504/1) 83.51% • ZIP compressed archive (8000/1) 16.49%
File name:	ComplaintDetails-1244065104-Nov-17.xlsb
File size:	97289
MD5:	cfee2afbf9c7456b62417ccf80e70009
SHA1:	2d43d6ad54fb33ce77467394e621963d528cc57f
SHA256:	0a7656fab771936b9586b8b90ebe9d38f34fa64d8e465f3f53c4df20f3c1ca44
SHA512:	0e34e23fc57dbaf8dabb479beded8c3b79b49d09f752472c68c924a5c1e4495d9dff24be0ea62652c4f1c5a46ff8c833bc17d72323fcb0105204c6c2c5146b62
SSDEEP:	1536:smepB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUNp:rc6EehCfCZpUHKGXbBKsiii
File Content Preview:	PK.....!...$7....~.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e2ea8aa4b4b4b4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "ComplaintDetails-1244065104-Nov-17.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:	

Indicators

Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-20:54:54.090042	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	190.14.37.101	192.168.2.22
12/02/21-20:55:36.529819	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	185.138.164.244	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 190.14.37.101
- 185.138.164.244

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	190.14.37.101	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:54:53.114980936 CET	0	OUT	GET /44532.8710387731.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 190.14.37.101 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:54:54.090042114 CET	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 19:54:53 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49170	185.138.164.244	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:55:36.236634016 CET	2	OUT	GET /44532.8710387731.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.138.164.244 Connection: Keep-Alive
Dec 2, 2021 20:55:36.529819012 CET	3	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 19:55:36 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: 2844 Parent PID: 596

General

Start time:	20:54:15
Start date:	02/12/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13f810000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 508 Parent PID: 2844

General

Start time:	20:55:01
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe ..\Tot1.ocx
Imagebase:	0xffe90000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 2956 Parent PID: 2844

General

Start time:	20:55:02
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe ..\Tot2.ocx
Imagebase:	0xffe90000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 2568 Parent PID: 2844

General

Start time:	20:55:02
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe ..\Tot3.ocx
Imagebase:	0xffe90000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly

Code Analysis