ID: 532936
Sample Name: ComplaintDetails-1244065104-Nov-17.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:01:17
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

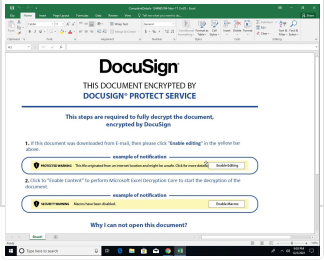
Windows Analysis Report ComplaintDetails-1244065104…

Overview

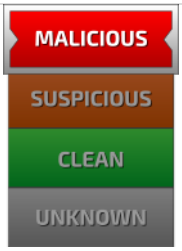
General Information

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

Most interesting Screenshot:



Detection



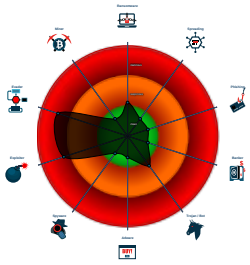
Hidden Macro 4.0

Score:	92
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
- Multi AV Scanner detection for doma…
- 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

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6316 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 1740 cmdline: regsvr32.exe ..\Tot1.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6344 cmdline: regsvr32.exe ..\Tot2.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6736 cmdline: regsvr32.exe ..\Tot3.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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

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

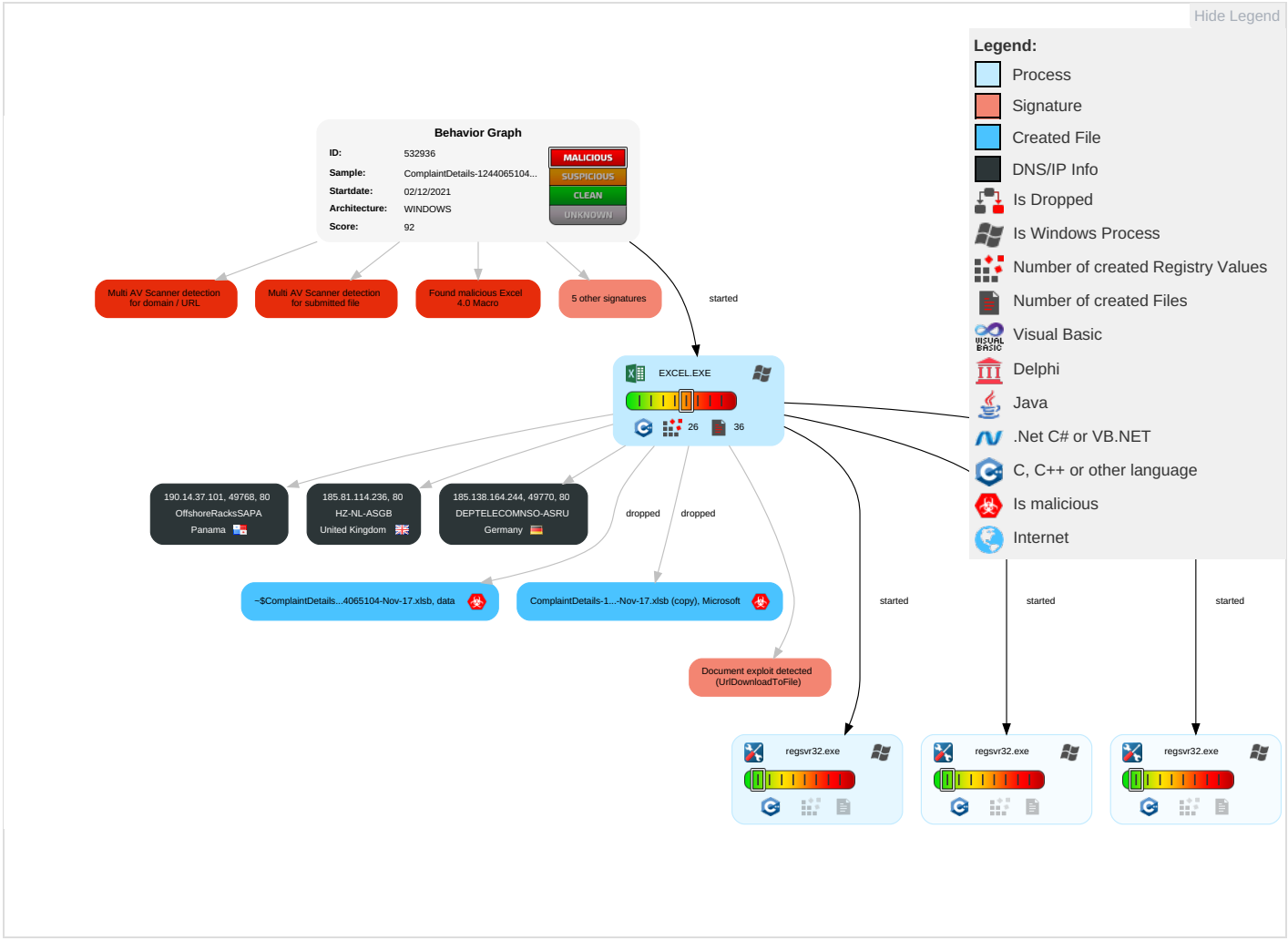
Found Excel 4.0 Macro with suspicious formulas

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	Remote Service Effects
Valid Accounts	Scripting 3	DLL Side-Loading 1	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 3	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorizatior
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	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatior
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 3	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
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	
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	

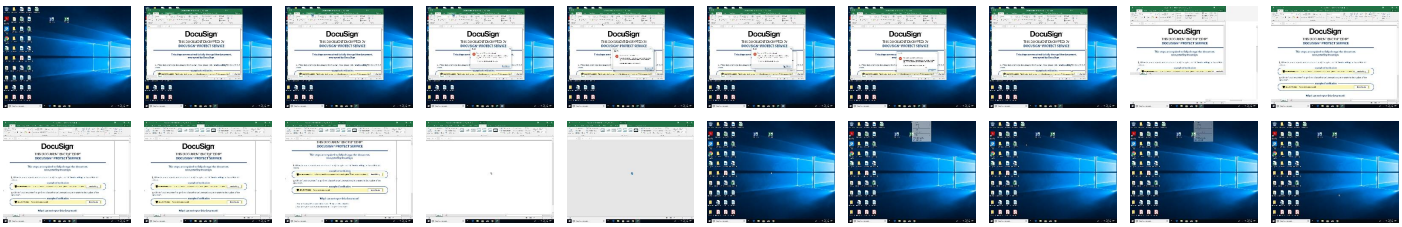
Behavior Graph

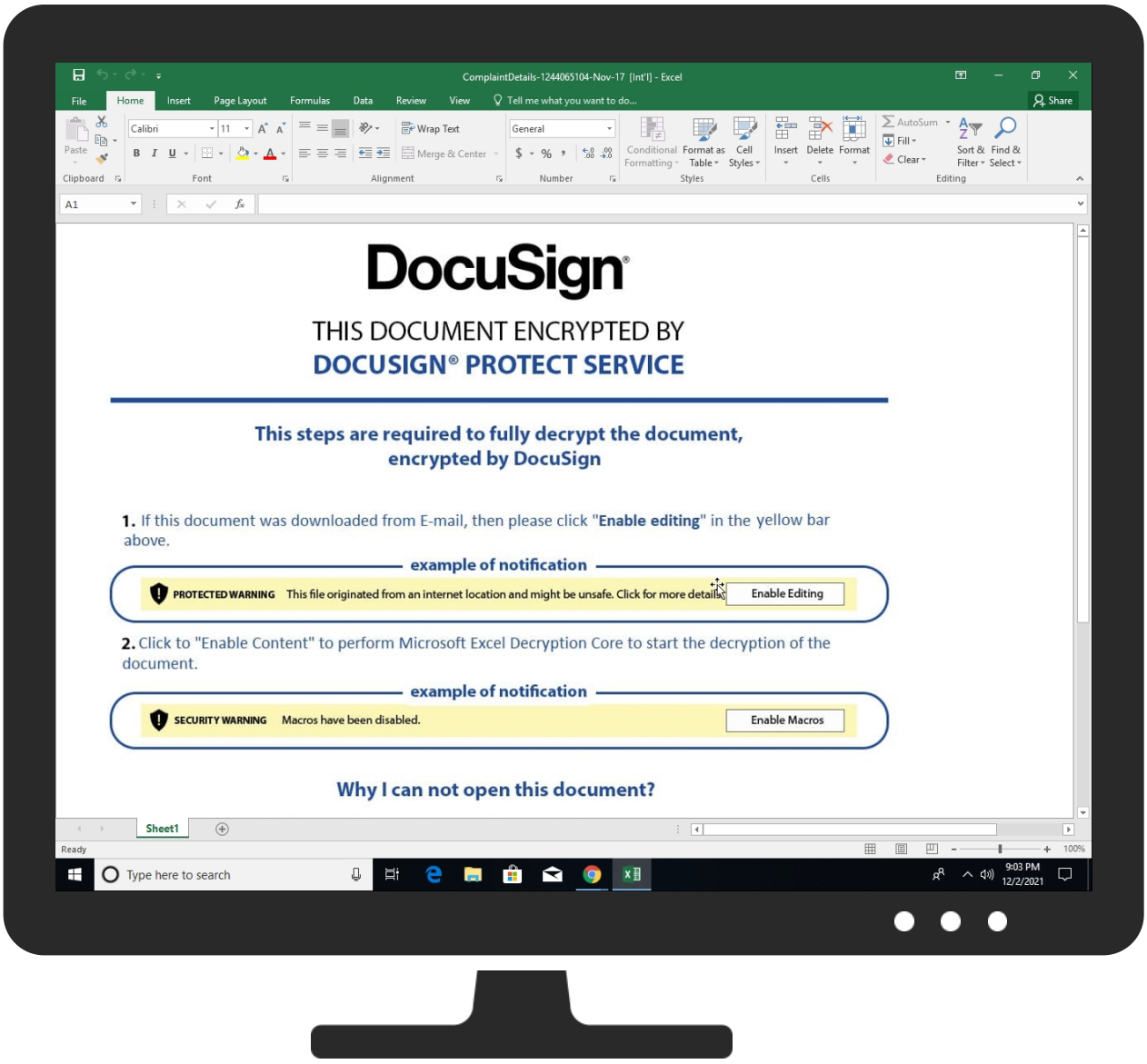


Screenshots

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	46%	Virustotal		Browse
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://https://substrate.office.comI9	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://185.138.164.244/	6%	Virustotal		Browse
http://185.138.164.244/	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://login.m	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://185.81.114.236/5563209-4053062332-1002	0%	Avira URL Cloud	safe	
http://schemas.open	0%	URL Reputation	safe	
http://190.14.37.101/44532.8765170139.datc	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://login.wind	0%	Avira URL Cloud	safe	
http://185.81.114.236/44532.8765170139.dat_	0%	Avira URL Cloud	safe	
http://190.14.37.101/44532.8765170139.datS	0%	Avira URL Cloud	safe	
http://190.14.37.101/44532.8765170139.datO	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://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://api.addins.store.officeppe.com/addinstemplatebW	0%	Avira URL Cloud	safe	
http://190.14.37.101/53321935-2125563209-4053062332-1002y	0%	Avira URL Cloud	safe	
http://https://management.azure.comh	0%	Avira URL Cloud	safe	
http://https://substrate.office.comc	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://190.14.37.101/A	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	URL Reputation	safe	
http://https://outlook.office.comR87	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://login.mcro	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
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:	21:01:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 22s
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 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:	17
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:	mal92.expl.evad.winXLSB@7/6@0/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
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
190.14.37.101	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	
185.138.164.244	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	• 185.138.164.244/445 32.8710387731.dat
185.81.114.236	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEPTELECOMNSO-ASRU	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	• 185.138.164.244
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 185.138.164.46
	10KaQvX7O7.exe	Get hash	malicious	Browse	• 185.138.164.150

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	V3fm0d84mp.exe	Get hash	malicious	Browse	• 185.138.164.150
	AqlmImmeey.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
	8aAG42oIjb.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
OffshoreRacksSAPA	ComplaintDetails-1244065104-Nov-17.xlsb	Get hash	malicious	Browse	• 190.14.37.101
	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

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\630E636C-6B0C-44EA-BF33-295CC8DCC16C	
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):	140352
Entropy (8bit):	5.3574479066156995
Encrypted:	false
SSDEEP:	1536:NcQIfgxrBdA3gBwtnQ9DQW+zUb4Ff7nXmvid1XiE6LWmE9:XuQ9DQW+zfXfH
MD5:	7041F82342CA3BB77AC6E03BBA053D21
SHA1:	662834DC1DBB8F985F52FBAF66F0232208FDEE8E
SHA-256:	2F4093011968416889176D93F5AA2288351E7015B11BAE20557FA3380805F079
SHA-512:	E25A46182FC97AC042D04E15891D6E96DC992FD45F38132A69D1C1EE14872D345DC917002F4B573AF7F6C78550BB9B7AE2C04AA928E2198FADD23C12DC90CF 2
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="2021-12-02T20:02:09">.. Build: 16.0.14729.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\227F60C2.jpg	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1098x988, frames 3
Category:	dropped
Size (bytes):	85681
Entropy (8bit):	7.915850776614707
Encrypted:	false
SSDEEP:	1536:wB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUw:Pc6EehCfCZpUHKGXbBKsiit
MD5:	4F100E2CEFED046B44EC799015B454EF
SHA1:	5149E5D1B5212C77B3548914E9B47D67B4BEA574
SHA-256:	D30B441AB0E88A1487F29A80D63E2A4865A3F5DF7854FB8359B354397F807E2C
SHA-512:	153581151434815CC17E88D587FF6A6AF8F7154B4A05146453A9814F662C68D79F1063BDD9F789A1DB2F5818D199EF600703F8BC35785B0705332EC231F35A14
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....'.....'#*" "*#>1++1>H<9<HWNNWmhm.....J.."..... .....".....q.[..+...*...K.... .....?.....g....6..)....=~.....w5.....7_.-.....k.../...;.....!.z%o..w!....,.....?...Gs?.]......C..P~i._.=. .`....{...w....."..-.....:...d.....;z7)...~g.....C....v..\..O.....0...v.....v... .....A...;.~Y.}.....MsC.~..5..?.;.....V7....G...b..~.....@.....O.}...o4.s_...z78.1.yl.. .X~.u..~..S....J..V~S..x.u~.. .....@....u..m....rGrf.P.._+Z..?AW..~..u.G.....o&.....9.0...H.Zx...M.y.[kW..o.....;.....z.....}v.m.. [R.i....R..m....+.J.....r6.P....|s..].vO._.}..K.]-V.U=9}.....W.....3.....G.t}Y

C:\Users\user\Desktop\74E50000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	97123
Entropy (8bit):	7.832617738018424
Encrypted:	false
SSDEEP:	1536:eB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUoIHz:pc6EehCfCZpUHKGXbBKsiiEHz
MD5:	6C82071E9F05B57CCD14462B49635CDF
SHA1:	CE666804DF7779E970D76D1AA64DB0F52543AEE2
SHA-256:	6C78C9C018C06F23A2936176B6D1BCBDCA054E21B86A4EC5007EE3ED62279EFE
SHA-512:	E8FB6BA91AFA9E74502D16834274E3F4E531980F1A00F0869DFAD0B9B65C221EE35D6CD6697B476C443690FC6ECCA522EFB67A47579C105D76F051F633916F15
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\74E50000: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

C:\Users\user\Desktop\74E50000:Zone.Identifier	
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 (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	97123
Entropy (8bit):	7.832617738018424
Encrypted:	false
SSDEEP:	1536:eB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUoIHz:pc6EehCfCZpUHKGXbBKsiiEHz
MD5:	6C82071E9F05B57CCD14462B49635CDF
SHA1:	CE666804DF7779E970D76D1AA64DB0F52543AEE2
SHA-256:	6C78C9C018C06F23A2936176B6D1BCBDCA054E21B86A4EC5007EE3ED62279EFE
SHA-512:	E8FB6BA91AFA9E74502D16834274E3F4E531980F1A00F0869DFAD0B9B65C221EE35D6CD6697B476C443690FC6ECCA522EFB67A47579C105D76F051F633916F15
Malicious:	**true**
Reputation:	low
Preview:	PK.....!..E.....~.....[Content_Types].xml ...(..... ....U.n.0....?..."......C..=.....q-1.H..l..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\~$ComplaintDetails-1244065104-Nov-17.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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

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

General

SHA256:	0a7656fab771936b9586b8b90ebe9d38f34fa64d8e465f3f53c4df20f3c1ca44
SHA512:	0e34e23fc57dbaf8dabb479beded8c3b79b49d09f752472c68c924a5c1e4495d9dff24be0ea62652c4f1c5a46ff8c833bc17d72323fcb0105204c6c2c5146b62
SSDEEP:	1536:smepB5SOqcuTUdehXyvl0f4CZpUcab2GFVbgPuDF7exsylBviKsUNp:rc6EehCfCZpUHKGXbBKsiii
File Content Preview:	PK.....!...$7....~.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

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:	
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	192.168.2.4	49768	190.14.37.101	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 21:02:11.903629065 CET	1286	OUT	GET /44532.8765170139.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: 190.14.37.101 Connection: Keep-Alive
Dec 2, 2021 21:02:12.878776073 CET	1287	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 20:02:12 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><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	192.168.2.4	49770	185.138.164.244	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 21:02:33.937803030 CET	1472	OUT	GET /44532.8765170139.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: 185.138.164.244 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 21:02:34.138546944 CET	1473	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 20:02:34 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: 6316 Parent PID: 800

General

Start time:	21:02:06
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:	0xa80000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 1740 Parent PID: 6316

General

Start time:	21:02:33
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe ..\Tot1.ocx
Imagebase:	0xcd0000
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: 6344 Parent PID: 6316

General

Start time:	21:02:34
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe ..\Tot2.ocx
Imagebase:	0xcd0000
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: 6736 Parent PID: 6316

General

Start time:	21:02:36
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32.exe ..\Tot3.ocx
Imagebase:	0xcd0000

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