

JOeSandbox Cloud BASIC



ID: 532593

Sample Name: counter-
1248368226.xls

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 14:26:54

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

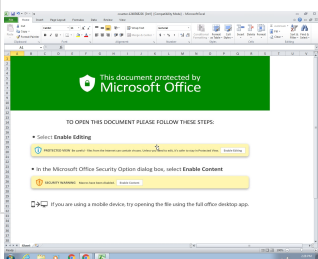
Table of Contents	2
Windows Analysis Report counter-1248368226.xls	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	4
Initial Sample	4
Dropped Files	4
Sigma Overview	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
Software Vulnerabilities:	5
System Summary:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	14
Static OLE Info	14
General	14
OLE File "counter-1248368226.xls"	14
Indicators	14
Summary	14
Document Summary	14
Streams	14
Macro 4.0 Code	14
Network Behavior	14
Network Port Distribution	15
TCP Packets	15
UDP Packets	15
DNS Queries	15
DNS Answers	15
HTTP Request Dependency Graph	15
HTTPS Proxied Packets	15
Code Manipulations	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: EXCEL.EXE PID: 2804 Parent PID: 596	16
General	16
File Activities	17
File Created	17
File Deleted	17
File Moved	17
Registry Activities	17

Key Created	17
Key Value Created	17
Key Value Modified	17
Analysis Process: regsvr32.exe PID: 2116 Parent PID: 2804	17
General	17
File Activities	17
Analysis Process: regsvr32.exe PID: 2920 Parent PID: 2804	17
General	17
File Activities	18
Analysis Process: regsvr32.exe PID: 1136 Parent PID: 2804	18
General	18
File Activities	18
Disassembly	18
Code Analysis	18

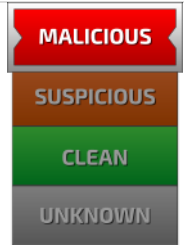
Windows Analysis Report counter-1248368226.xls

Overview

General Information

Sample Name:	counter-1248368226.xls
Analysis ID:	532593
MD5:	30a0db47a66a3d..
SHA1:	c852a219defe8ab.
SHA256:	bdd97906934a97..
Infos:	
Most interesting Screenshot:	

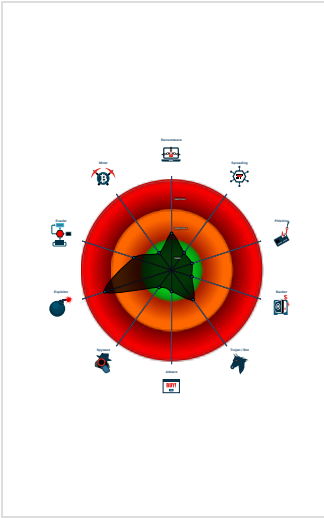
Detection

	
Hidden Macro 4.0	
Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Office document tries to convince vi...
Multi AV Scanner detection for subm...
Antivirus detection for URL or domain
Sigma detected: Microsoft Office Pr...
Document exploit detected (process...
Document exploit detected (UrlDown...
Yara detected hidden Macro 4.0 in E...
Yara signature match
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: 2804 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
•  regsvr32.exe (PID: 2116 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\besta.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
•  regsvr32.exe (PID: 2920 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestb.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
•  regsvr32.exe (PID: 1136 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
▪ cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
counter-1248368226.xls	SUSP_Excel4Macro_Auto Open	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x1deaa:\$s1: Excel 0x1ef56:\$s1: Excel 0x34cf:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A
counter-1248368226.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\counter-1248368226.xls	SUSP_Excel4Macro_Auto Open	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	0x0:\$header_docf: D0 CF 11 E0 0x1deaa:\$s1: Excel 0x1ef56:\$s1: Excel 0x34cf:\$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\counter-1248368226.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	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

Antivirus detection for URL or domain

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)

HIPS / PFW / Operating System Protection Evasion:

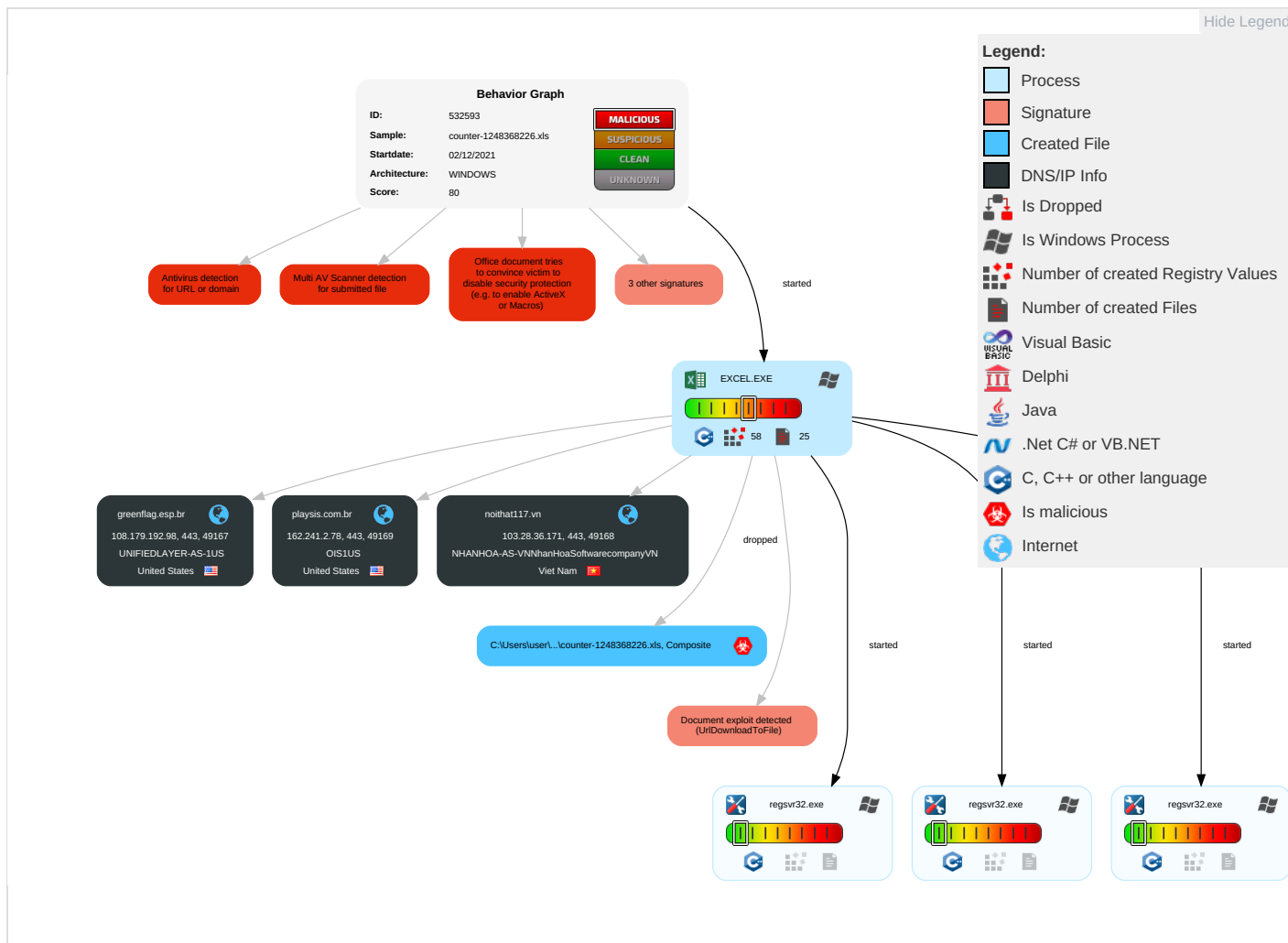


Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Scripting 1	Path Interception	Process Injection 2	Disable or Modify Tools 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 2	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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

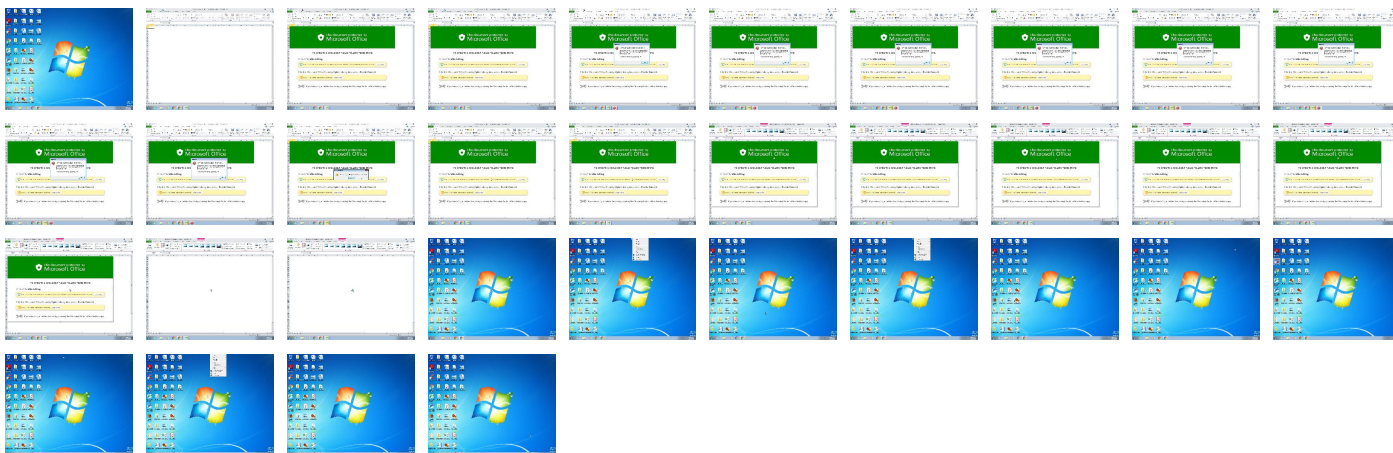
Behavior Graph

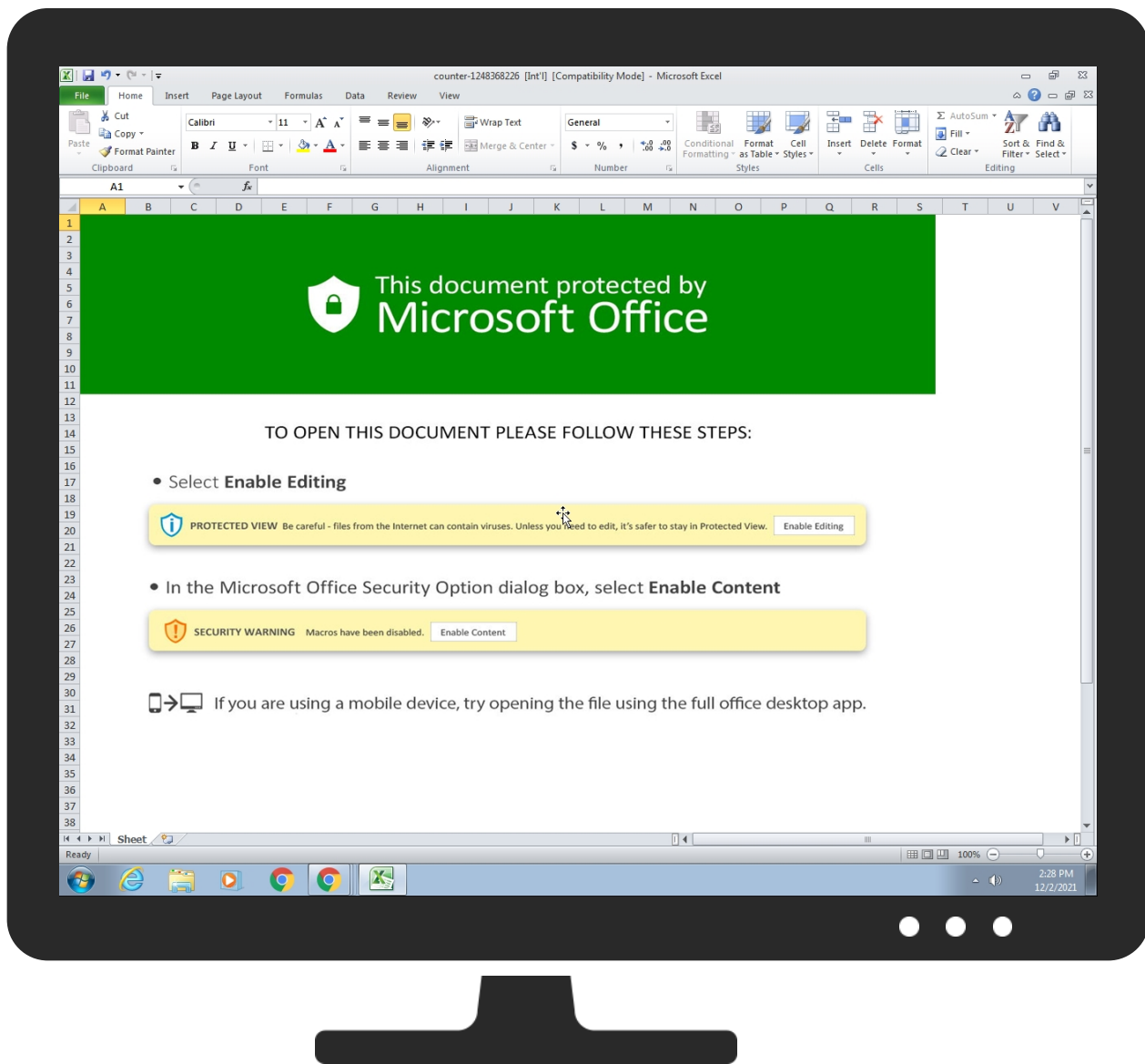


Screenshots

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
counter-1248368226.xls	41%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://playsis.com.br/viderJ	100%	Avira URL Cloud	malware	
http://https://noithat117.vn/TSh7GBelR/tiynh.htmlfs7y	0%	Avira URL Cloud	safe	
http://schemas.openformatrg/drawml/2006/spreadsheetD	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://playsis.com.br/qJSi	100%	Avira URL Cloud	malware	
http://schemas.openformatrg/package/2006/content-t	0%	URL Reputation	safe	
http://https://playsis.com	0%	Avira URL Cloud	safe	
http://https://greenflag.esp.br/	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://greenflag.esp.br/~	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qJSL1BN5V/tiynh.html117.vn/TSh7GBelR/tiynh.htmlink	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redirect/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://playsis.com.br/qJSL117.	100%	Avira URL Cloud	malware	
http://schemas.open	0%	URL Reputation	safe	
http://https://playsis.cre	0%	Avira URL Cloud	safe	
http://https://noithat117.vn/TSh7GBelR/tiynh.html	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://schemas.openformatrg/package/2006/r	0%	URL Reputation	safe	
http://https://greenflag.esp.br/yulNdRbM/tiynh.htmltv7y	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qJSL1BN5V/tiynh.html3W(y	100%	Avira URL Cloud	malware	
http://https://greenflag.esp.br/yulNdRbM/tiynh.html	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qJSL1B.b	100%	Avira URL Cloud	malware	
http://https://noithat117.vn/	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qhtt	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://playsis.com.boi	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qJSL1BN5V/tiynh.html	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://playsis.com.br/qJSL1BNt	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
greenflag.esp.br	108.179.192.98	true	false		unknown
playsis.com.br	162.241.2.78	true	false		unknown
noithat117.vn	103.28.36.171	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://noithat117.vn/TSh7GBelR/tiynh.html	false	Avira URL Cloud: safe	unknown
http://https://greenflag.esp.br/yulNdRbM/tiynh.html	false	Avira URL Cloud: safe	unknown
http://https://playsis.com.br/qJSL1BN5V/tiynh.html	true	Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.2.78	playsis.com.br	United States		26337	OIS1US	false
108.179.192.98	greenflag.esp.br	United States		46606	UNIFIEDLAYER-AS-1US	false
103.28.36.171	noithat117.vn	Viet Nam		131353	NHANHOA-AS-VNNhanHoaSoftwarecompan yVN	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532593
Start date:	02.12.2021
Start time:	14:26:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	counter-1248368226.xls
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:	8
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:	mal80.expl.winXLS@7/4@3/3
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: .xls • 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

Time	Type	Description
14:27:28	API Interceptor	373x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.2.78	#Uacac#Uc801 #Ud488#Ubaa9 #Ub9ac#Uc2a4#Ud2b8.exe	Get hash	malicious	Browse	www.entrep iparaodigi tal.com/jdkn/? 1b0=I3 SbQcfk5mKn cCcQGw+gNu eSmbNJxTZB bu+zAfDoz/ ZWf2NQTBtv 1zSdSMYJHd n3WlwE&mJB HHf=B0DPf0 S8lbot
108.179.192.98	counter-119221000.xls	Get hash	malicious	Browse	
	counter-119221000.xls	Get hash	malicious	Browse	
	tr.xls	Get hash	malicious	Browse	
	tr.xls	Get hash	malicious	Browse	
	counter-1389180325.xls	Get hash	malicious	Browse	
	counter-1389180325.xls	Get hash	malicious	Browse	
103.28.36.171	211094.exe	Get hash	malicious	Browse	www.nhada t9chu.com/ iae2/?Cb=t lljdtXg+6s s6GeFkxkNX /Gta+EnXEK PHxZQNK05o pTQPj/ZdNF PdnHw1EJZh rtLdJv1ORZ 2Rg==&uVjH =yVCTVb0XT 254cnY

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
noithat117.vn	counter-119221000.xls	Get hash	malicious	Browse	103.28.36.171
	counter-119221000.xls	Get hash	malicious	Browse	103.28.36.171
	tr.xls	Get hash	malicious	Browse	103.28.36.171
	tr.xls	Get hash	malicious	Browse	103.28.36.171
	counter-1389180325.xls	Get hash	malicious	Browse	103.28.36.171
	counter-1389180325.xls	Get hash	malicious	Browse	103.28.36.171
playsis.com.br	counter-119221000.xls	Get hash	malicious	Browse	162.241.2.78
	counter-119221000.xls	Get hash	malicious	Browse	162.241.2.78
	tr.xls	Get hash	malicious	Browse	162.241.2.78
	tr.xls	Get hash	malicious	Browse	162.241.2.78
	counter-1389180325.xls	Get hash	malicious	Browse	162.241.2.78
	counter-1389180325.xls	Get hash	malicious	Browse	162.241.2.78
greenflag.esp.br	counter-119221000.xls	Get hash	malicious	Browse	108.179.192.98
	counter-119221000.xls	Get hash	malicious	Browse	108.179.192.98
	tr.xls	Get hash	malicious	Browse	108.179.192.98
	tr.xls	Get hash	malicious	Browse	108.179.192.98
	counter-1389180325.xls	Get hash	malicious	Browse	108.179.192.98
	counter-1389180325.xls	Get hash	malicious	Browse	108.179.192.98

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OIS1US	a2SyRyTizn.exe	Get hash	malicious	Browse	162.241.20 3.110
	TSmtlLEeJ.exe	Get hash	malicious	Browse	162.241.20 3.110
	counter-119221000.xls	Get hash	malicious	Browse	162.241.2.78
	counter-119221000.xls	Get hash	malicious	Browse	162.241.2.78
	tr.xls	Get hash	malicious	Browse	162.241.2.78
	tr.xls	Get hash	malicious	Browse	162.241.2.78
	counter-1389180325.xls	Get hash	malicious	Browse	162.241.2.78
	counter-1389180325.xls	Get hash	malicious	Browse	162.241.2.78
	PURCHASE ORDER HECTRO.xlsx	Get hash	malicious	Browse	162.241.85.81
	chase.xls	Get hash	malicious	Browse	162.241.2.167
	chase.xls	Get hash	malicious	Browse	162.241.2.167

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	private-1915056036.xls	Get hash	malicious	Browse	162.241.2.167
	private-1915056036.xls	Get hash	malicious	Browse	162.241.2.167
	private-1910485378.xls	Get hash	malicious	Browse	162.241.2.167
	private-1910485378.xls	Get hash	malicious	Browse	162.241.2.167
	Amended Order.xlsx	Get hash	malicious	Browse	162.241.2.151
	aLTbT3KJXg.exe	Get hash	malicious	Browse	192.185.147.203
	qWeAgF7WNO.exe	Get hash	malicious	Browse	192.185.147.203
	Page_1of3#Ud83d#Udce0.html	Get hash	malicious	Browse	162.241.70.204
	INV8897.xlsx	Get hash	malicious	Browse	162.241.2.97
UNIFIEDLAYER-AS-1US	CU-6431 report.xlsm	Get hash	malicious	Browse	162.240.9.126
	CU-6431 report.xlsm	Get hash	malicious	Browse	162.240.9.126
	DkX9HVJTmi.exe	Get hash	malicious	Browse	108.167.135.122
	Shipping report -17420.xlsx	Get hash	malicious	Browse	162.241.169.32
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	162.240.9.126
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	162.240.9.126
	INVOICE.exe	Get hash	malicious	Browse	162.214.80.6
	img20048901738_Pago.pdf.exe	Get hash	malicious	Browse	192.185.115.3
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	162.241.126.156
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	162.241.126.156
	New order documents. pdf.....exe	Get hash	malicious	Browse	108.179.232.76
	part-1500645108.xlsb	Get hash	malicious	Browse	162.241.62.201
	img20048901740_Pago.pdf.exe	Get hash	malicious	Browse	192.185.115.3
	part-1500645108.xlsb	Get hash	malicious	Browse	162.241.62.201
	shedy.exe	Get hash	malicious	Browse	162.241.218.172
	product list.xlsx	Get hash	malicious	Browse	162.241.218.178
	accounts...exe	Get hash	malicious	Browse	192.185.164.148
	New product of Aluminium Profile.exe	Get hash	malicious	Browse	192.185.84.191
	BL. AWSMUNDAR3606-21.exe	Get hash	malicious	Browse	162.241.148.56
	draft_inv dec21.exe	Get hash	malicious	Browse	162.241.120.147

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	CU-6431 report.xlsm	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	DHL Original shipping Document_pdf.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	New Price List.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	Hotel Guest List.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	IRQ2107798.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	AWB.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	FILE_915494026923219.xlsm	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	IRQ2107797.ppam	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	part-1500645108.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	invoice template 33142738819.docx	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	item-40567503.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	FILE_464863409880121918.xlsm	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	item-107262298.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	item-1202816963.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	counter-119221000.xls	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	box-1688169224.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	box-1689035414.xlsb	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171
	survey-1805824485.xls	Get hash	malicious	Browse	162.241.2.78 108.179.192.98 103.28.36.171

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\DAB5.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsaTILPltI2N81HRQjIORgt7RQ//W1XR9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	>.....

C:\Users\user\AppData\Local\Temp\~DF3B4EA5BD8BBCDF15.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.9736664173647833
Encrypted:	false
SSDEEP:	768:9kxKpb8rGyrMPe3q7Q0XV5xtezEs/68/dgALINp:9oKpb8rGyrMPe3q7Q0XV5xtezEsi8/dh
MD5:	193AED4E8225F55CE53F3DE42895D51E
SHA1:	35C2A28EB87E87B40275737D4EE569B5D45BF237
SHA-256:	92B61AE08A4A89E9086400FC634F2A39313F3D685BDAF4810059B265CED6A12B

C:\Users\user1\AppData\Local\Temp\~DF3B4EA5BD8BBCDF15.TMP	
SHA-512:	C13251F8EB2434D37697F95B56EA9DF4B44AFC4A1FBBF45F1B765926C7E4AF45A91D0DB5EE835A5B109EB90106D2B368821E0A55D07C72A582856EE260D29CB D
Malicious:	false
Reputation:	low
Preview:	

C:\Users\user1\AppData\Local\Temp\~DFEAC2A307FBF2A788.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B07134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	

C:\Users\user1\Desktop\counter-1248368226.xls		
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE	
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Nov 30 06:43:37 2021, Security: 0	
Category:	dropped	
Size (bytes):	132608	
Entropy (8bit):	6.276322779310474	
Encrypted:	false	
SSDEEP:	3072:bKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgRjYVceeiE/RzPQUu/zLOQy:bKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgzx	
MD5:	79614FAA563C6EF0EB88F17D98CD485F	
SHA1:	30A312B65370CBC0B211967B46E4B4B9610CA873	
SHA-256:	14852BCA3BFE3C4B276B639C26EED9A65C7754150015EC16EF323C8408D66F2C	
SHA-512:	E68DE46993A2215DB3BB111B926C0F880D54D4E78E7AF4F48094190CD7633BBE9DC8873817226676B39C6EB200A7DBE30EC45DD7D32D886FC2784F3455A55BC	
Malicious:	true	
Yara Hits:	- Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user1\Desktop\counter-1248368226.xls, Author: John Lambert @JohnLaTwC - Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user1\Desktop\counter-1248368226.xls, Author: Joe Security	
Reputation:	low	
Preview:	>.....ZO.....\p.....user.8.=.....B.....a.....=.....=.....Ve18.....X.@....."1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.	

Static File Info

General	
File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Nov 30 06:43:37 2021, Security: 0
Entropy (8bit):	6.275934021202815
TrID:	- Microsoft Excel sheet (30009/1) 78.94% - Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	counter-1248368226.xls
File size:	132608

General	
MD5:	30a0db47a66a3d3173457755bb166529
SHA1:	c852a219defe8ab726b72f8792386e35428b46dc
SHA256:	bdd97906934a97d1081e68ac8f71c98a169c4af705c17b73b69b3649df216885
SHA512:	ca0fb9713e25d2c3f1fa312c9318801ee7f97d4f0873501bd05de98bc0dc25020d7ae5f7fd88368dcdbc261c4a4d86a9ccc4c376ae85a014945b4cc7f572cb5d
SSDEEP:	3072:LKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgRjYVceeiE/RzPQUu/zLOQj:LKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgzE
File Content Preview:	>.....

File Icon

	
Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "counter-1248368226.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2021-11-30 06:43:37
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 14:27:48.784358025 CET	192.168.2.22	8.8.8.8	0x3c72	Standard query (0)	greenflag.esp.br	A (IP address)	IN (0x0001)
Dec 2, 2021 14:27:50.456291914 CET	192.168.2.22	8.8.8.8	0x6c3	Standard query (0)	noithat117.vn	A (IP address)	IN (0x0001)
Dec 2, 2021 14:27:52.924587011 CET	192.168.2.22	8.8.8.8	0x313b	Standard query (0)	playsis.com.br	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 14:27:48.804148912 CET	8.8.8.8	192.168.2.22	0x3c72	No error (0)	greenflag.esp.br		108.179.192.98	A (IP address)	IN (0x0001)
Dec 2, 2021 14:27:50.773180962 CET	8.8.8.8	192.168.2.22	0x6c3	No error (0)	noithat117.vn		103.28.36.171	A (IP address)	IN (0x0001)
Dec 2, 2021 14:27:53.086635113 CET	8.8.8.8	192.168.2.22	0x313b	No error (0)	playsis.com.br		162.241.2.78	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- greenflag.esp.br
- noithat117.vn
- playsis.com.br

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	108.179.192.98	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:27:49 UTC	0	OUT	GET /yulNdRbM/tjynh.html 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: greenflag.esp.br Connection: Keep-Alive
2021-12-02 13:27:50 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 13:27:49 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	103.28.36.171	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:27:51 UTC	0	OUT	GET /TSh7GBelR/tiynh.html 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: noithat117.vn Connection: Keep-Alive
2021-12-02 13:27:52 UTC	0	IN	HTTP/1.1 200 OK Connection: close Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Thu, 02 Dec 2021 13:27:52 GMT Server: LiteSpeed Alt-Svc: quic=":443"; ma=2592000; v="43,46", h3-Q043=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-25=":443"; ma=2592000, h3-27=":443"; ma=2592000

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	162.241.2.78	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:27:53 UTC	1	OUT	GET /qJSL1BN5V/tiynh.html 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: playasis.com.br Connection: Keep-Alive
2021-12-02 13:27:54 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 13:27:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2804 Parent PID: 596

General

Start time:	14:27:17
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:	0x13f870000

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 Moved

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 2116 Parent PID: 2804

General

Start time:	14:27:28
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datoplbesta.ocx
Imagebase:	0xff9c0000
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: 2920 Parent PID: 2804

General

Start time:	14:27:28
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datoplbestb.ocx
Imagebase:	0xff9c0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 1136 Parent PID: 2804

General

Start time:	14:27:29
Start date:	02/12/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx
Imagebase:	0xff9c0000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis