ID: 532593
Sample Name: counter-1248368226.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:34:57
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

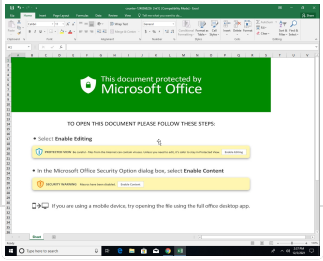
Windows Analysis Report counter-1248368226.xls

Overview

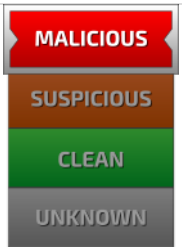
General Information

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

Most interesting Screenshot:



Detection



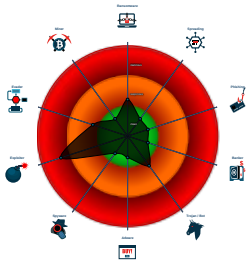
Hidden Macro 4.0

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…
- Tries to load missing DLLs
- Uses a known web browser user age…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 2172 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6380 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\besta.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6404 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestb.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6424 cmdline: "C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
counter-1248368226.xls	SUSP_Excel4Macro_AutoOpen	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 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_AutoOpen	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 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)

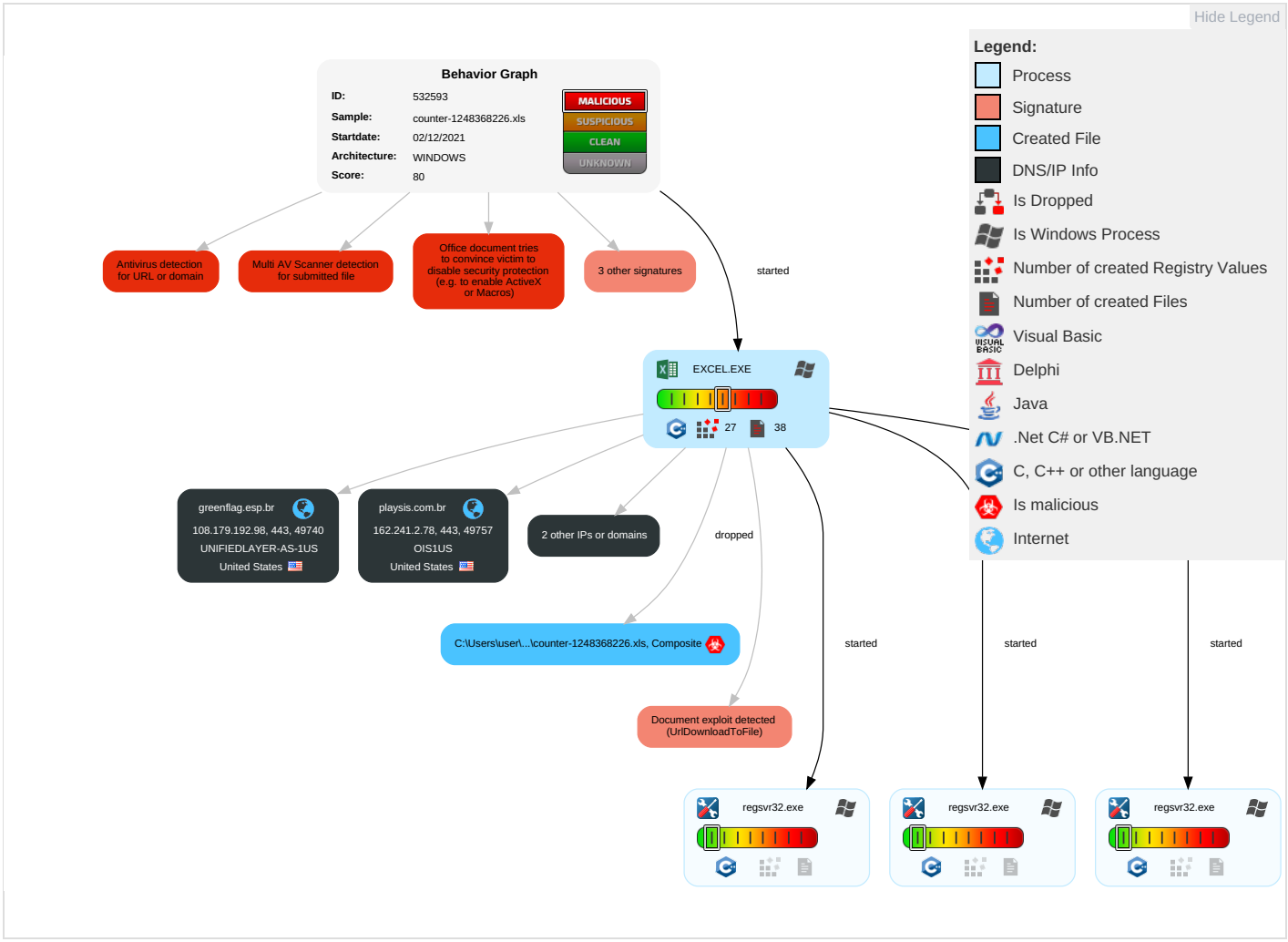
HIPS / PFW / Operating System Protection Evasion:

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	Remote Service Effects	Im
Valid Accounts	Scripting 1	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 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mo Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	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 1	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 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	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

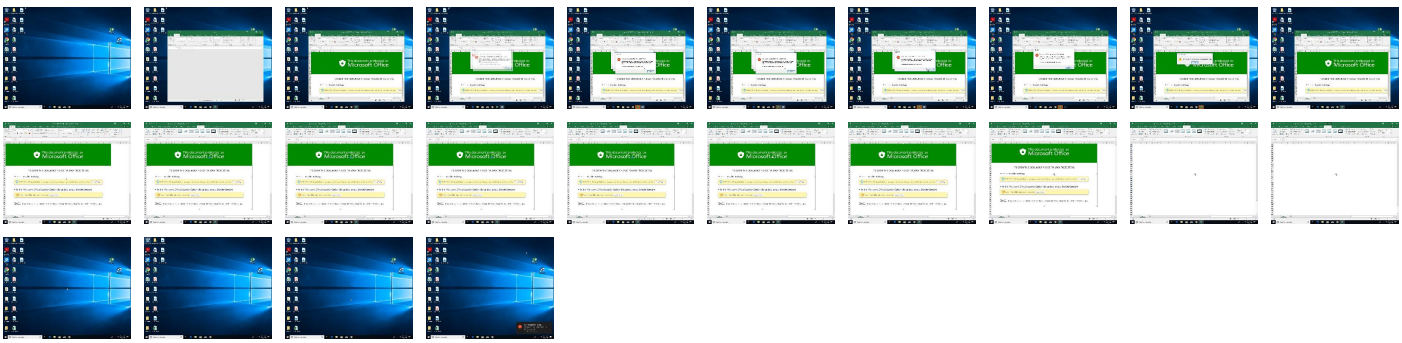
Behavior Graph

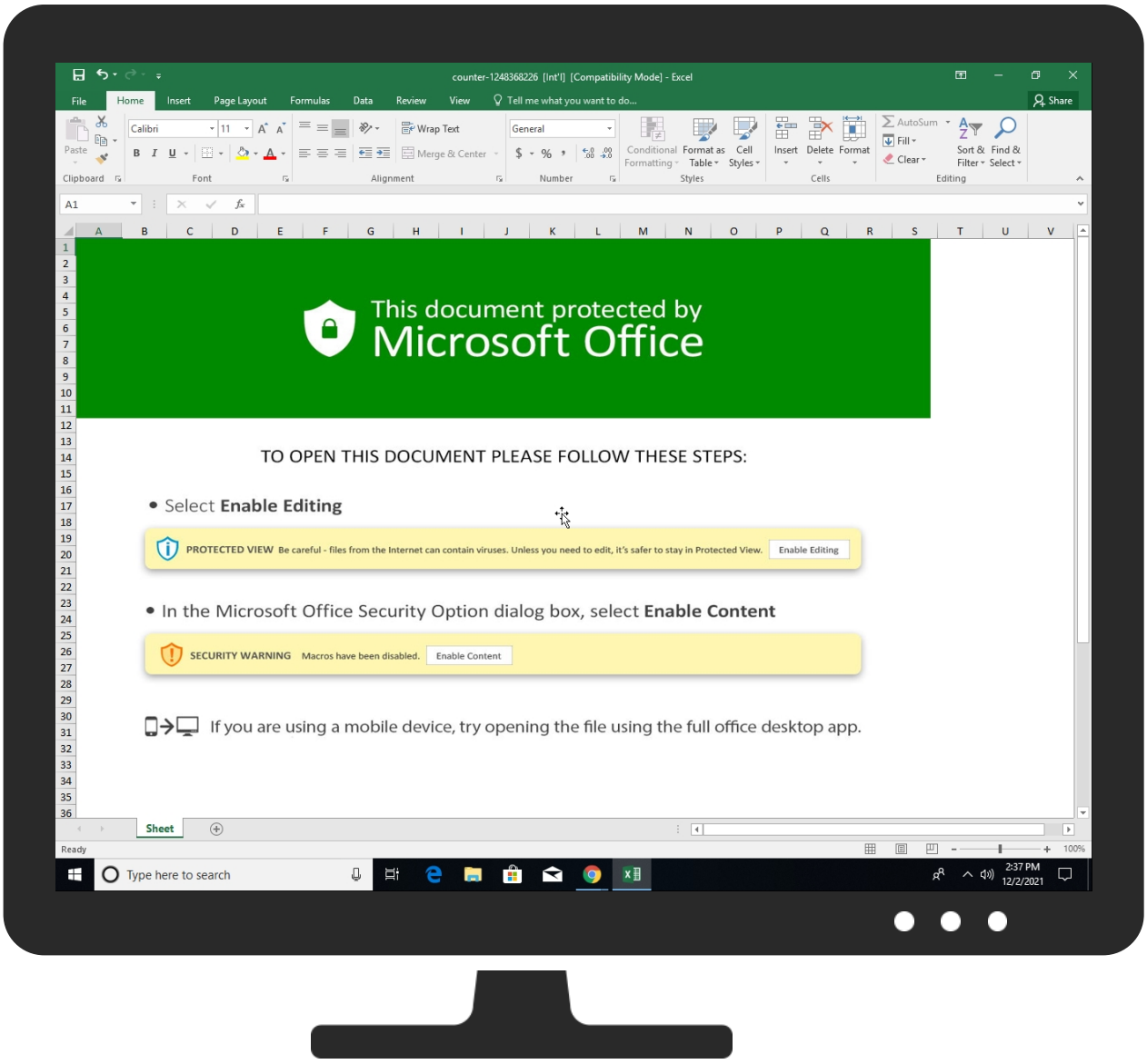


Screenshots

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

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
greenflag.esp.br	1%	Virustotal		Browse
playsis.com.br	1%	Virustotal		Browse
noithat117.vn	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://incidents.diagnosticssdf.office.comq	0%	Avira URL Cloud	safe	
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	
http://schemas.open	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com8Q	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://noithat117.vn/TSh7GBeIR/tiynh.htmlx	0%	Avira URL Cloud	safe	
http://https://playsis.com.br/qJSL1BN5V/tiynh.html	100%	Avira URL Cloud	malware	
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://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://substrate.office.comk	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://noithat117.vn/N_k	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comMBI	0%	Avira URL Cloud	safe	
http://https://greenflag.esp.br/yuINdRbM/tiynh.html	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://api.cortana.aiL	0%	Avira URL Cloud	safe	
http://https://api.cortana.aiP	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://greenflag.esp./	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.msom	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	• 1%, Virustotal, Browse	unknown
playsis.com.br	162.241.2.78	true	false	• 1%, Virustotal, Browse	unknown
noithat117.vn	103.28.36.171	true	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://playsis.com.br/qJSL1BN5V/tiynh.html	true	• Avira URL Cloud: malware	unknown
http://https://greenflag.esp.br/yuINdRbM/tiynh.html	false	• Avira URL Cloud: safe	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-VNNhanHoaSoftwarecompanyVN	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532593
Start date:	02.12.2021
Start time:	14:34:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	counter-1248368226.xls
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:	30
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@7/5@3/4
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

No simulations

Joe Sandbox View / Context

IPs

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.entreiparaodigital.com/jdkn/?1b0=l3SbQcfk5mKncCcQGw+gNueSmbNJxTZBbu+zAfDoz/ZWf2NQtBtv1zSdSMyJHdn3WlwE&mJBHHf=B0DPf0S8Ibot
108.179.192.98	counter-1248368226.xls	Get hash	malicious	Browse	
	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.nhadat9chu.com/iae2/?Cb=tlljdtxg+6ss6GeFkxkNX/Gta+EnXEkPHxZQNKO5opTQPj/ZdNFPdnHw1EJZhrtLdJv1ORZ2Rg==&uVjH=yVCTVb0XT254cnY

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
noithat117.vn	counter-1248368226.xls	Get hash	malicious	Browse	• 103.28.36.171
	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-1248368226.xls	Get hash	malicious	Browse	• 162.241.2.78
	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	counter-1248368226.xls	Get hash	malicious	Browse	• 162.241.2.78
	a2SyRyTizn.exe	Get hash	malicious	Browse	• 162.241.203.110
	TSmtIL1EeJ.exe	Get hash	malicious	Browse	• 162.241.203.110
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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
UNIFIEDLAYER-AS-1US	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	ukmxWblFcs.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	Narudzba.0953635637.PDF.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	Orden de compra.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	EmployeeAssessment.html	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	Tender SN980018277 & SN9901827 Signed Copy.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	Rifc8lYWh7.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	umA9dNEzIh.exe	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
	Rifc8lYWh7.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	umA9dNEzIh.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	rU6eiJaifC.exe	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
	Kqn63gUZFq.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	837375615376.dll	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	NTS_eTaxInvoice 1-12-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	837375615376.dll	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	lzJWJgZhPc.exe	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	• 162.241.2.78 • 108.179.192.98 • 103.28.36.171
	SMK_EFT_BILLPAY.html	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\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\62A0C483-7525-45C3-9021-D9D0BAA7B779	
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):	140163
Entropy (8bit):	5.358154429516242
Encrypted:	false
SSDEEP:	1536:ScQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:auQ9DQW+zJXfH
MD5:	194ED8DC6E6E9FC0B894576EBA1030DA
SHA1:	91C12CDE373DF4700BD254667AA2DD25AA4990B2
SHA-256:	7244698AEBF849E11174ADB5FBDC6E582C2475D4FC986692C5F3C02B84D437B2
SHA-512:	71AF6D56CD8AD0816F51A4523C04E664B8B942ABDE8F2329289855534B8559D67D592ED8E854CC1DE1E0C66D337B5EE23DFB322EF258AD9F5D4A448407F2FFC A
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="2021-12-02T13:36:00">.. Build: 16.0.14715.30527-->.. <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\A032B20.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A032B20.tmp	
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB3 9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Temp\~DF852A535A08A1983B.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	2.974047404887019
Encrypted:	false
SSDEEP:	768:nkxKpb8rGYrMPe3q7Q0XV5xtezEs/68/dgALlNp:noKpb8rGYrMPe3q7Q0XV5xtezEsi8/dh
MD5:	6235D05472679068C67F48FDCF00B91D
SHA1:	8259DEBBFCAFDA24C2FEF013F0AF4F840B35B847
SHA-256:	9E32E87680CDB684D3D2BB47426999E90B6914D554B84ECBEE63A527D778E059
SHA-512:	50820596D0D1F9404EE4F8732EE1E9A1B7AB26BA1F344DF0F72974859C1056A0157D1F867782270DA8269DF6D6C874E23EC02EF8DB3C0DBC0613E840710BB632
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFC6022B2B101620FE.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\Desktop\counter-1248368226.xls	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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):	6.2763302357105974
Encrypted:	false
SSDEEP:	3072:xKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgRJyVceeiE/RzPQUu/zLOQo:xKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgz/
MD5:	0B49C3AF7CA3F0B4C6C0706CA1C27D40
SHA1:	AB90F79F25B6EA9E44CD6A927CA0CDC7E7C089CA
SHA-256:	31EB146BFD8F5B35A2509F6A22B57CC89D17591012B087D3A21379AD35EE06BB
SHA-512:	0430DBF9CEF861C21148F1DA1734A3EA4F69A0A669867E68861C91510BB63DABC29CAC362E768043E9679B6C5C26706CF0B0819E85AFE24B9929B1DCA867067
Malicious:	**true**

C:\Users\user\Desktop\counter-1248368226.xls	
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\counter-1248368226.xls, Author: John Lambert @JohnLaTwC • Rule: JoeSecurity_HiddenMacro, Description: Yara detected hidden Macro 4.0 in Excel, Source: C:\Users\user\Desktop\counter-1248368226.xls, Author: Joe Security
Preview:	.....>..... .....ZO..... .....\.p....pratesh.=. 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
MD5:	30a0db47a66a3d3173457755bb166529
SHA1:	c852a219defe8ab726b72f8792386e35428b46dc
SHA256:	bdd97906934a97d1081e68ac8f71c98a169c4af705c17b73b69b3649df216885
SHA512:	ca0fb9713e25d2c3f1fa312c9318801ee7f97d4f0873501bd05de98bc0dc25020d7ae5f7fd88368dcbdc261c4a4d86a9ccc4c376ae85a014945b4cc7f572cb5d
SSDEEP:	3072:LKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgRJyVceeiE/RzPQUu/zLOQj:LKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgzE
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

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:	

Summary	
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 14:36:05.943691015 CET	192.168.2.5	8.8.8.8	0x6c94	Standard query (0)	greenflag.esp.br	A (IP address)	IN (0x0001)
Dec 2, 2021 14:36:07.408467054 CET	192.168.2.5	8.8.8.8	0xaff6	Standard query (0)	noithat117.vn	A (IP address)	IN (0x0001)
Dec 2, 2021 14:36:09.831341982 CET	192.168.2.5	8.8.8.8	0x9fd8	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 14:36:05.961409092 CET	8.8.8.8	192.168.2.5	0x6c94	No error (0)	greenflag.esp.br		108.179.192.98	A (IP address)	IN (0x0001)
Dec 2, 2021 14:36:07.426022053 CET	8.8.8.8	192.168.2.5	0xaff6	No error (0)	noithat117.vn		103.28.36.171	A (IP address)	IN (0x0001)
Dec 2, 2021 14:36:09.979106903 CET	8.8.8.8	192.168.2.5	0x9fd8	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	192.168.2.5	49740	108.179.192.98	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:36:06 UTC	0	OUT	GET /yuINdRbM/tiynh.html 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: greenflag.esp.br Connection: Keep-Alive
2021-12-02 13:36:07 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 13:36:06 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	192.168.2.5	49753	103.28.36.171	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:36:07 UTC	0	OUT	GET /TSh7GBeIR/tiynh.html 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: noithat117.vn Connection: Keep-Alive
2021-12-02 13:36:09 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 13:36:09 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	192.168.2.5	49757	162.241.2.78	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-12-02 13:36:10 UTC	1	OUT	GET /qJSL1BN5V/tiynh.html 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: playsis.com.br Connection: Keep-Alive
2021-12-02 13:36:11 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 13:36:10 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: 2172 Parent PID: 792

General

Start time:	14:35:58
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:	0x1390000
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 Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6380 Parent PID: 2172

General

Start time:	14:36:11
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\besta.ocx
Imagebase:	0x11a0000
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: 6404 Parent PID: 2172

General

Start time:	14:36:12
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\bestb.ocx
Imagebase:	0x11a0000
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: 6424 Parent PID: 2172

General

Start time:	14:36:12
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\regsvr32.exe" C:\Datop\bestc.ocx
Imagebase:	0x11a0000
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