ID: 499734
Sample Name: 1701667874-10042021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:37:38
Date: 08/10/2021
Version: 33.0.0 White Diamond

Table of Contents

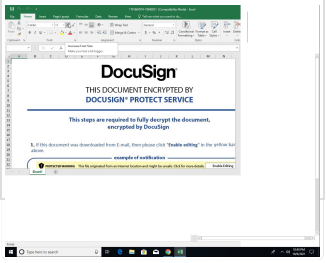
Windows Analysis Report 1701667874-10042021.xls

Overview

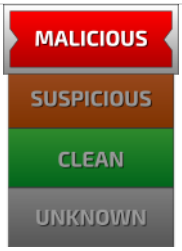
General Information

Sample Name:	1701667874-10042021.xls
Analysis ID:	499734
MD5:	1dc3a1c0972a9e..
SHA1:	808311a0752295..
SHA256:	9828f899790d150.
Tags:	xls xls
Infos:	

Most interesting Screenshot:



Detection



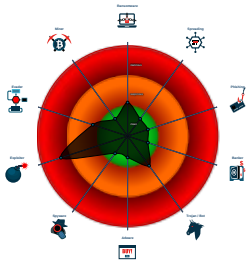
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Potential document exploit detected…
- Tries to load missing DLLs
- Tries to connect to HTTP servers, b…
- Document contains an embedded VB…
- Document contains embedded VBA …

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 472 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 2872 cmdline: regsvr32 -silent ..\Celod.wac MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5972 cmdline: regsvr32 -silent ..\Celod.wac1 MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4868 cmdline: regsvr32 -silent ..\Celod.wac2 MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
1701667874-10042021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

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)

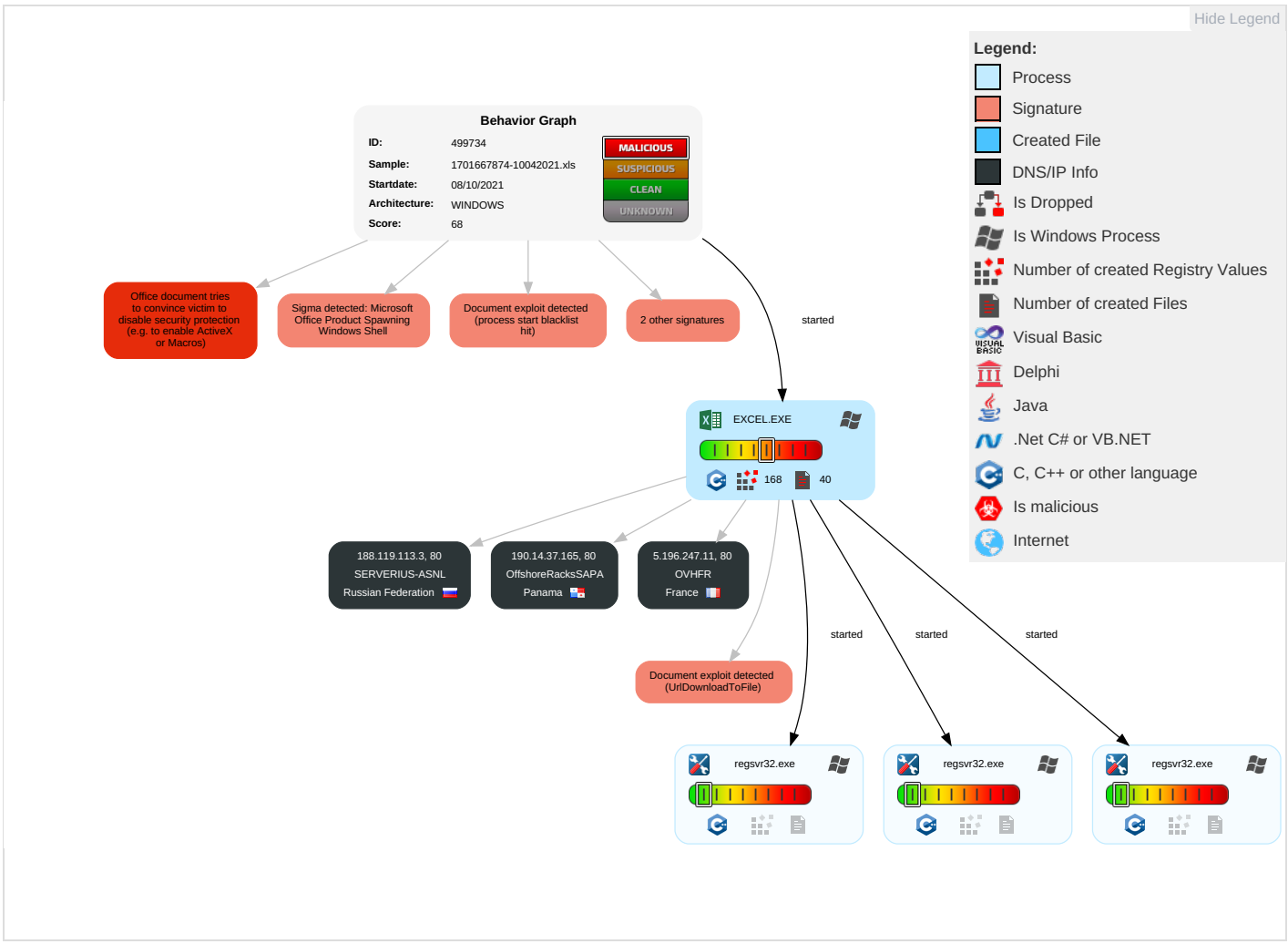
HIPS / PFW / Operating System Protection Evasion:

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	Ir
Valid Accounts	Scripting 2	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M S P
Default Accounts	Exploitation for Client Execution 2 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C B F
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		M A R o

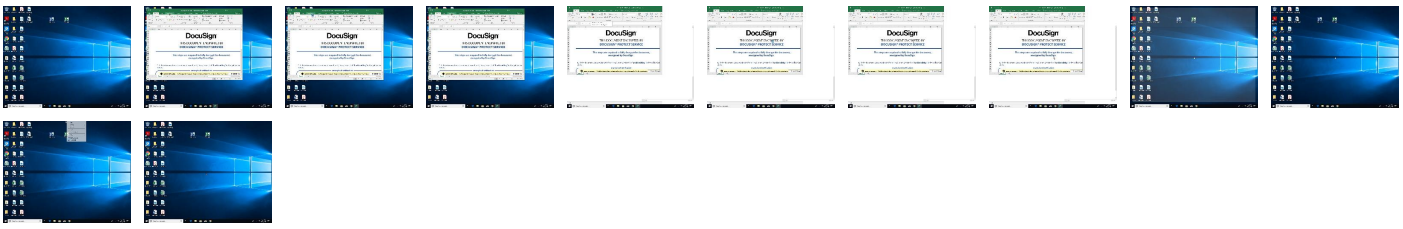
Behavior Graph

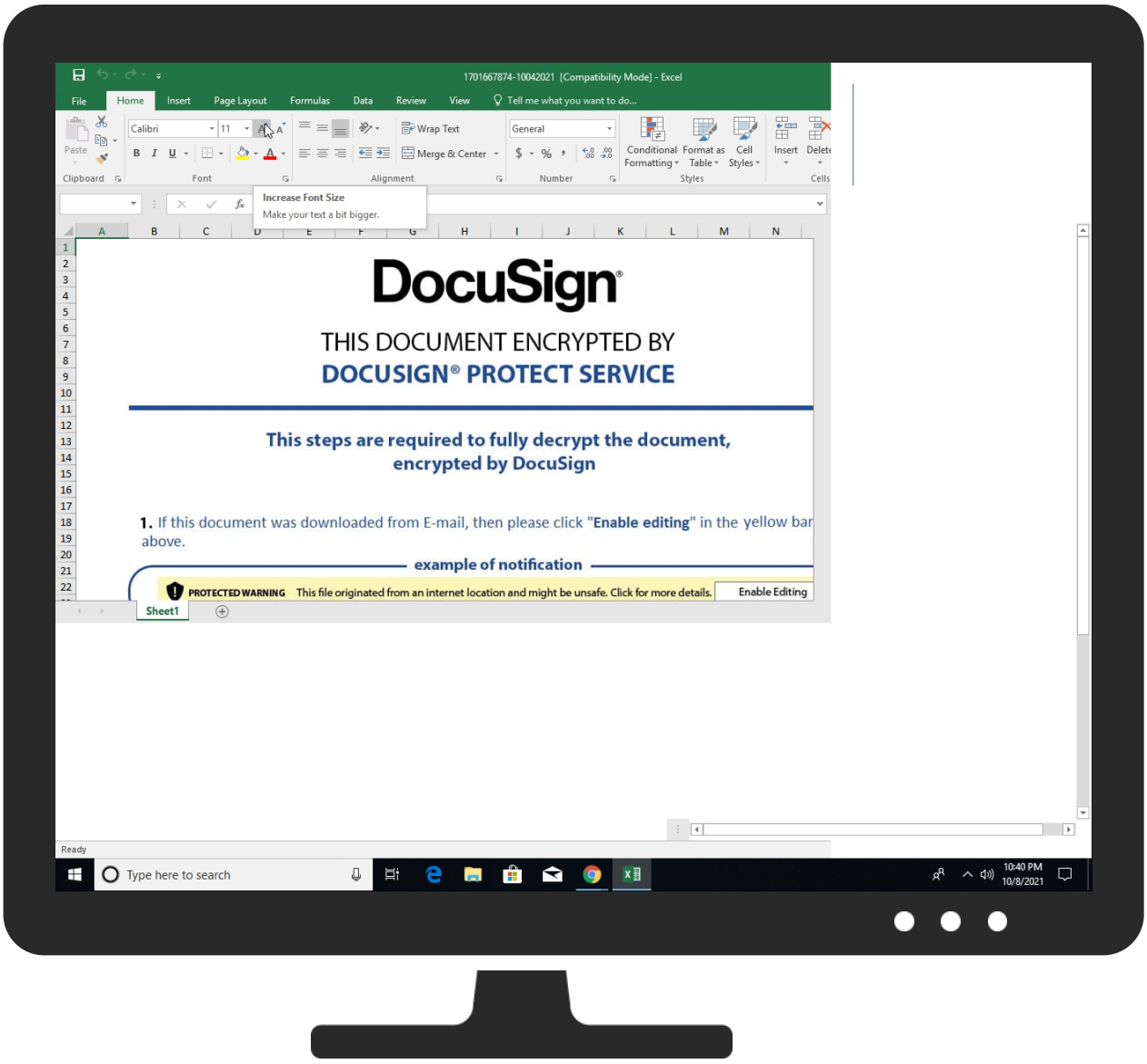


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://188.119.113.3/	4%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://188.119.113.3/	0%	Avira URL Cloud	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	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://api.aadrm.com	0%	Virustotal		Browse
http://https://api.aadrm.com	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://5.196.247.11/	4%	Virustotal		Browse
http://5.196.247.11/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	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
5.196.247.11	unknown	France		16276	OVHFR	false
190.14.37.165	unknown	Panama		52469	OffshoreRacksSAPA	false
188.119.113.3	unknown	Russian Federation		50673	SERVERIUS-ASNL	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	499734
Start date:	08.10.2021
Start time:	22:37:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 30s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	1701667874-10042021.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:	19
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:	mal68.expl.winXLS@7/3@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: .xls • Changed system and user locale, location and keyboard layout to English - United States • 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
5.196.247.11	173536952-10042021.xls	Get hash	malicious	Browse	• 5.196.247.11/44473.7079048611.dat
190.14.37.165	173536952-10042021.xls	Get hash	malicious	Browse	• 190.14.37.165/44473.7079048611.dat
188.119.113.3	173536952-10042021.xls	Get hash	malicious	Browse	• 188.119.113.3/44473.7079048611.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERIUS-ASNL	1701667874-10042021.xls	Get hash	malicious	Browse	• 188.119.113.3
	GlPWvtggPp.exe	Get hash	malicious	Browse	• 193.38.55.46
	z8dCygeB6f.exe	Get hash	malicious	Browse	• 188.119.113.208
	173536952-10042021.xls	Get hash	malicious	Browse	• 188.119.113.3
	hFRBBl9qJL	Get hash	malicious	Browse	• 46.249.32.215
	qVoV2KOkEU	Get hash	malicious	Browse	• 46.249.32.215
	gkfL4Bz8D0	Get hash	malicious	Browse	• 46.249.32.215
	Fy6PrO6OOe	Get hash	malicious	Browse	• 46.249.32.215
	Trainer v9.2.4.exe	Get hash	malicious	Browse	• 45.67.228.152
	03tjfO4HU9.exe	Get hash	malicious	Browse	• 45.67.231.218
	34e76d8a68c1eefd5681eb51a19019d189323f646c789.exe	Get hash	malicious	Browse	• 188.119.113.86
	JNk46WKTxo.exe	Get hash	malicious	Browse	• 45.67.228.118
	Document_1752244602-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149
	Document_1752244602-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149
	Document_1752244602-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149
	qbot5.xlsx	Get hash	malicious	Browse	• 193.38.54.149
	qbot5.xlsx	Get hash	malicious	Browse	• 193.38.54.149
	qbot5.xlsx	Get hash	malicious	Browse	• 193.38.54.149
	Document_85143683-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149
	Document_5153204-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149
OVHFR	1701667874-10042021.xls	Get hash	malicious	Browse	• 5.196.247.11
	FOL_JDHD98373_AMAZON_COMPROBANTE_FISCAL_DIGITAL_0398309_JDHSGGS.html	Get hash	malicious	Browse	• 144.217.13 9.163
	BROCATELLE.exe	Get hash	malicious	Browse	• 178.32.63.50
	yutrre123.exe	Get hash	malicious	Browse	• 213.186.33.5
	dec.exe	Get hash	malicious	Browse	• 213.186.33.5
	5DRyQNWb8e.exe	Get hash	malicious	Browse	• 51.195.57.236
	Contract-No-AJ-1343CL-REFERENCE-837373HH YAAHYSBDDS3736362_OCTOBER-2021.vbs	Get hash	malicious	Browse	• 178.32.63.50
	P. OFERTA 211008 Balearia Eurolineas Maritimas, S.A.exe	Get hash	malicious	Browse	• 94.23.221.28
	SCAN_COP.EXE	Get hash	malicious	Browse	• 51.210.156.152
	CONFIRM_.EXE	Get hash	malicious	Browse	• 51.210.156.152
	MV ROCKET_PDA.exe	Get hash	malicious	Browse	• 37.187.131.150
	6pDnJNQuXp	Get hash	malicious	Browse	• 51.161.7.116
	fh6FJ4ntlE	Get hash	malicious	Browse	• 51.161.7.116
	w7l28fLnhL	Get hash	malicious	Browse	• 51.161.7.116
	Vw1TY7nUmj	Get hash	malicious	Browse	• 51.161.7.116
	HqFa1ntiY8	Get hash	malicious	Browse	• 51.161.7.116
	0WefzeoV6X	Get hash	malicious	Browse	• 51.161.7.116
	YrNB27LHmu	Get hash	malicious	Browse	• 51.161.7.116
	bZEi1V3BCt	Get hash	malicious	Browse	• 51.161.7.116
	k0pLFMJMbp.dll	Get hash	malicious	Browse	• 54.39.106.25
OffshoreRacksSAPA	1701667874-10042021.xls	Get hash	malicious	Browse	• 190.14.37.165
	AMLRPT_257035367.xls	Get hash	malicious	Browse	• 190.14.37.238
	AMLRPT_1428592311.xls	Get hash	malicious	Browse	• 190.14.37.238
	AMLRPT_819011139.xls	Get hash	malicious	Browse	• 190.14.37.238
	AMLRPT_1428592311.xls	Get hash	malicious	Browse	• 190.14.37.238
	AMLRPT_819011139.xls	Get hash	malicious	Browse	• 190.14.37.238
	Document_1680405650-10062021.xls	Get hash	malicious	Browse	• 190.14.37.107
	Document_1680405650-10062021.xls	Get hash	malicious	Browse	• 190.14.37.107
	Document_748968552-10062021.xls	Get hash	malicious	Browse	• 190.14.37.107
	173536952-10042021.xls	Get hash	malicious	Browse	• 190.14.37.165
	UdQiakT3q5.xls	Get hash	malicious	Browse	• 190.14.37.187
	UdQiakT3q5.xls	Get hash	malicious	Browse	• 190.14.37.187
	Compensation-54975366-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-54975366-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	CompensationClaim-1630636598-09282021.xls	Get hash	malicious	Browse	• 190.14.37.187
	CompensationClaim-1033191014-09282021.xls	Get hash	malicious	Browse	• 190.14.37.187
	xls.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-1214892625-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-2100058996-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178
	Compensation-1657705079-09272021.xls	Get hash	malicious	Browse	• 190.14.37.178

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\A0633F26-EC8F-47DE-85C4-78BC1E11A6E5	
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):	138049
Entropy (8bit):	5.359443903800741
Encrypted:	false
SSDEEP:	1536:PcQIKNZrBdA3gBwfnQ9DQW+zBY34Zzi7nXboOidXVE6LWME9:LWQ9DQW+zbXa1
MD5:	C552E0D51C224C027D2A104736A3E120
SHA1:	2A8018013752906D3B1B937966E495EAF5A79212
SHA-256:	206A9EF4269C039E220EEDDC2D05A8B92F379141DDAE853D27B713F02E9EE9E9
SHA-512:	357E7BA89076E0F8E3633ABE36B317556AD525F12CDB2EB3798ECC2A0A662651A0DA29F6A2EE416FFFC9C8AB21008085018883B7224D0345D188EACEC6BA7ED F
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="2021-10-08T20:38:33">.. Build: 16.0.14604.30525-->.. <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\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	170164
Entropy (8bit):	4.366004047943934
Encrypted:	false
SSDEEP:	1536:f7nyfzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3oKmmy:f7yc8WpFpKKHHedydFeo+oQLUlPoK0
MD5:	CCDCF9F32EA30275AA12EE0C5F1E1C97
SHA1:	6D6AF50F39A813A584ADB72E86950EA4E658C020
SHA-256:	8B3131D27BFBF1D5F49B26CBBBE2767FCD46DC42C5BE70F3210369511168751B
SHA-512:	89B55DD510B18BDF8C338B279E44C8B9A2CD5CAD382A5085679CB995A72C2605C15C3473D11E5341B9AD91B65F2EEC15F47B39962BD5D56DBE8E31EECFC6A 80
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....$.....$..... .....d.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..l ... ..4!...!...!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,..,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8...8...9..l9...9..4:...:...:..`:...;.. (<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....l...B.....$..... ....x...l.....T..... ....

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	15676
Entropy (8bit):	4.563631392944346
Encrypted:	false
SSDEEP:	192:y/d4xlA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLdZ:x38xesT20lheZ3waE5D7qxlxkxZ
MD5:	31DB0BA1731116648AAAEC8C7090B256
SHA1:	C2E16B85FD0E20CB1DE4ECA308F9E41C2E75039E
SHA-256:	2ECD8535AAC73B8A846B8CD78FC707B380E20F12459713222FA241D8DFBCBB64

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
SHA-512:	44625FC207DB7307E5625B677BB2D27E9747A017EA132E6AEB89726762FB26FE8F3DD811D8D2DEE61C1602491809998455C806FC69DD2A1537FDF2B6FBD9D43
Malicious:	false
Reputation:	low
Preview:	MSFT.....A.....1..... .....d.....\.....H...4.....0... .....x.....x. .....$!.....0...+.....{...{...{.....P.....H.....$!.....~...~..0....P.,..... ..0.....%!.....H..".....H.....(.....@.....P.....0.....`.....p...X... ..... ...qdD..I.....E.....F.....B.....`..d.....E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<WI.....\.1Y.....k...U....."....."....|...K ..a...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Test, Last Saved By: Test, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Mon Oct 4 09:34:12 2021, Security: 0
Entropy (8bit):	7.07736722605419
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	1701667874-10042021.xls
File size:	132608
MD5:	1dc3a1c0972a9e32d88e85d1cf8f2c65
SHA1:	808311a07522956f55bf842749083e199b0f04c6
SHA256:	9828f899790d150360e0a3f78f3eb3b758417644bc16896aeb411e2af9e8ea4b
SHA512:	9bd8112044f2ca4f11861a50773c4cd98ce69bb04f523c4168c35481431eb2347a4ecb0e5c806217fdb89a977283168236046ebbdc0d7e556456b6ed5ba575db
SSDEEP:	3072:Sk3hOdsylKlgxopeiBNhZFGzE+cL2kdAxc6YehWfGdtUHKGDbpmsii/+u6ssC06+:Sk3hOdsylKlgxopeiBNhZF+E+W2kdAxX
File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "1701667874-10042021.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:	Test
Last Saved By:	Test
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-10-04 08:34:12
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 with VBA

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/08/21-22:31:07.677315	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
10/08/21-22:31:11.677211	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
10/08/21-22:31:19.027109	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
10/08/21-22:31:29.867071	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
10/08/21-22:31:34.047252	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22
10/08/21-22:31:40.057139	ICMP	399	ICMP Destination Unreachable Host Unreachable			186.148.101.114	192.168.2.22

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 8, 2021 22:38:49.388036966 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 472 Parent PID: 800

General

Start time:	22:38:30
Start date:	08/10/2021
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:	0x140000
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

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 2872 Parent PID: 472

General

Start time:	22:39:38
Start date:	08/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac
Imagebase:	0x110000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 5972 Parent PID: 472

General

Start time:	22:39:39
Start date:	08/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac1
Imagebase:	0x110000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 4868 Parent PID: 472

General

Start time:	22:39:39
Start date:	08/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac2
Imagebase:	0x110000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis