

ID: 499734
Sample Name: 1701667874-10042021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:30:15
Date: 08/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 1701667874-10042021.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
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 5
Software Vulnerabilities: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
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
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 11
Static OLE Info 12
General 12
OLE File "1701667874-10042021.xls" 12
Indicators 12
Summary 12
Document Summary 12
Streams with VBA 12
Streams 12
Network Behavior 12
Snort IDS Alerts 12
Network Port Distribution 12
TCP Packets 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: EXCEL.EXE PID: 2016 Parent PID: 596 13
General 13
File Activities 13
File Created 13
File Deleted 13
File Moved 13
File Written 13
Registry Activities 13
Key Created 13
Key Value Created 13
Analysis Process: regsvr32.exe PID: 2184 Parent PID: 2016 13
General 13
Analysis Process: regsvr32.exe PID: 1612 Parent PID: 2016 14
General 14
Analysis Process: regsvr32.exe PID: 2528 Parent PID: 2016 14

Copyright Joe Security LLC 2021

General 14
Disassembly 14
Code Analysis 14

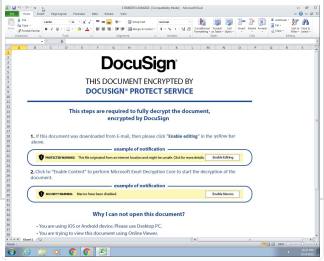
Windows Analysis Report 1701667874-10042021.xls

Overview

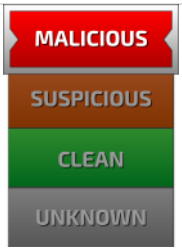
General Information

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

Most interesting Screenshot:



Detection



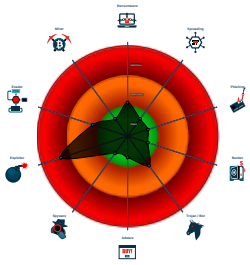
Hidden Macro 4.0

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

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2016 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 2184 cmdline: regsvr32 -silent ..\Celod.wac MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1612 cmdline: regsvr32 -silent ..\Celod.wac1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2528 cmdline: regsvr32 -silent ..\Celod.wac2 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **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: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Copyright Joe Security LLC 2021

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:



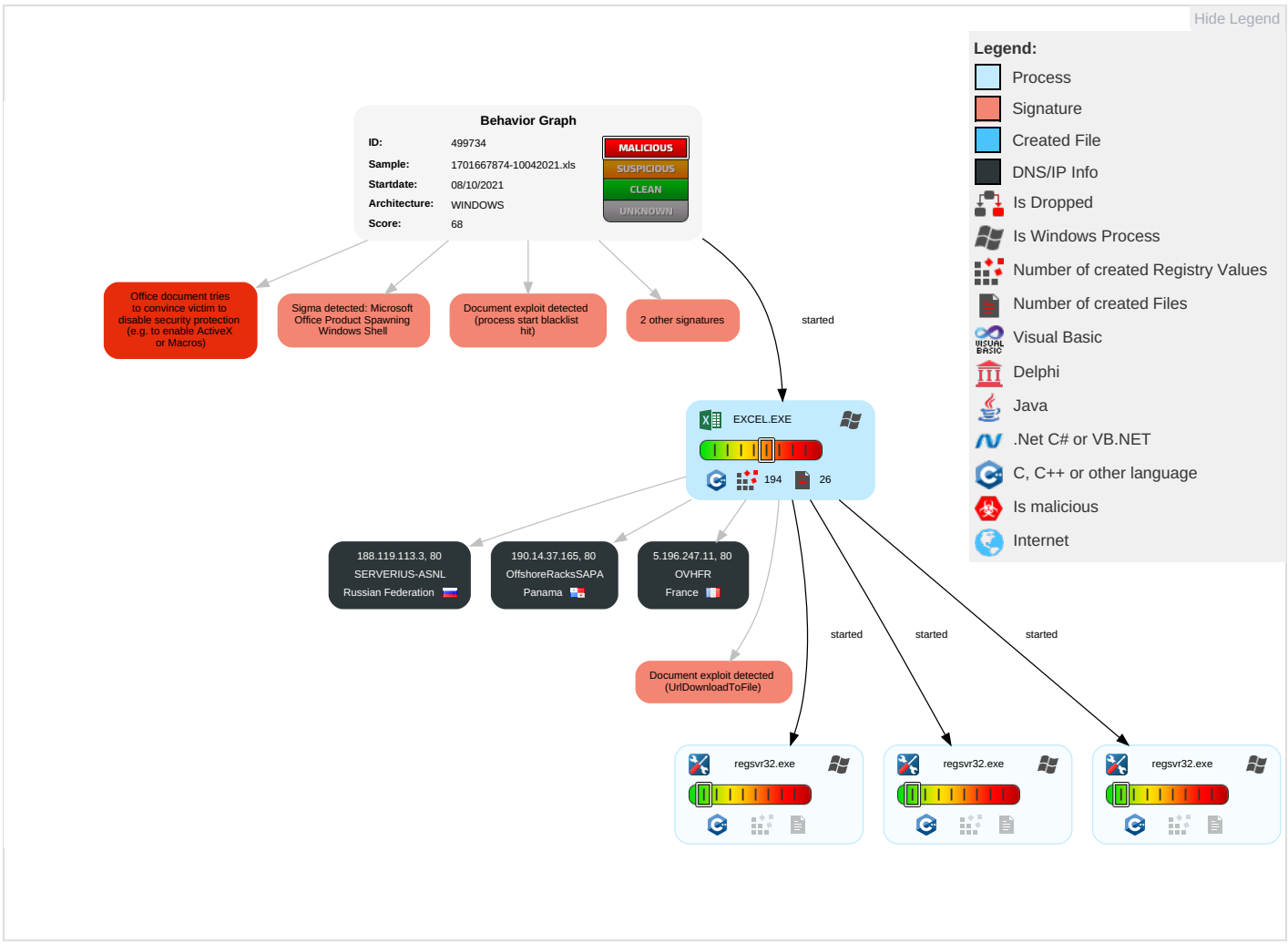
Yara detected hidden Macro 4.0 in Excel

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	Impac
Valid Accounts	Scripting 2	Path Interception	Process Injection 1	Disable or Modify Tools 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	Modify Systen Partitic
Default Accounts	Exploitation for Client Execution 2 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 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	Device Lockou
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 2	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	Delete Device Data

Behavior Graph

Copyright Joe Security LLC 2021

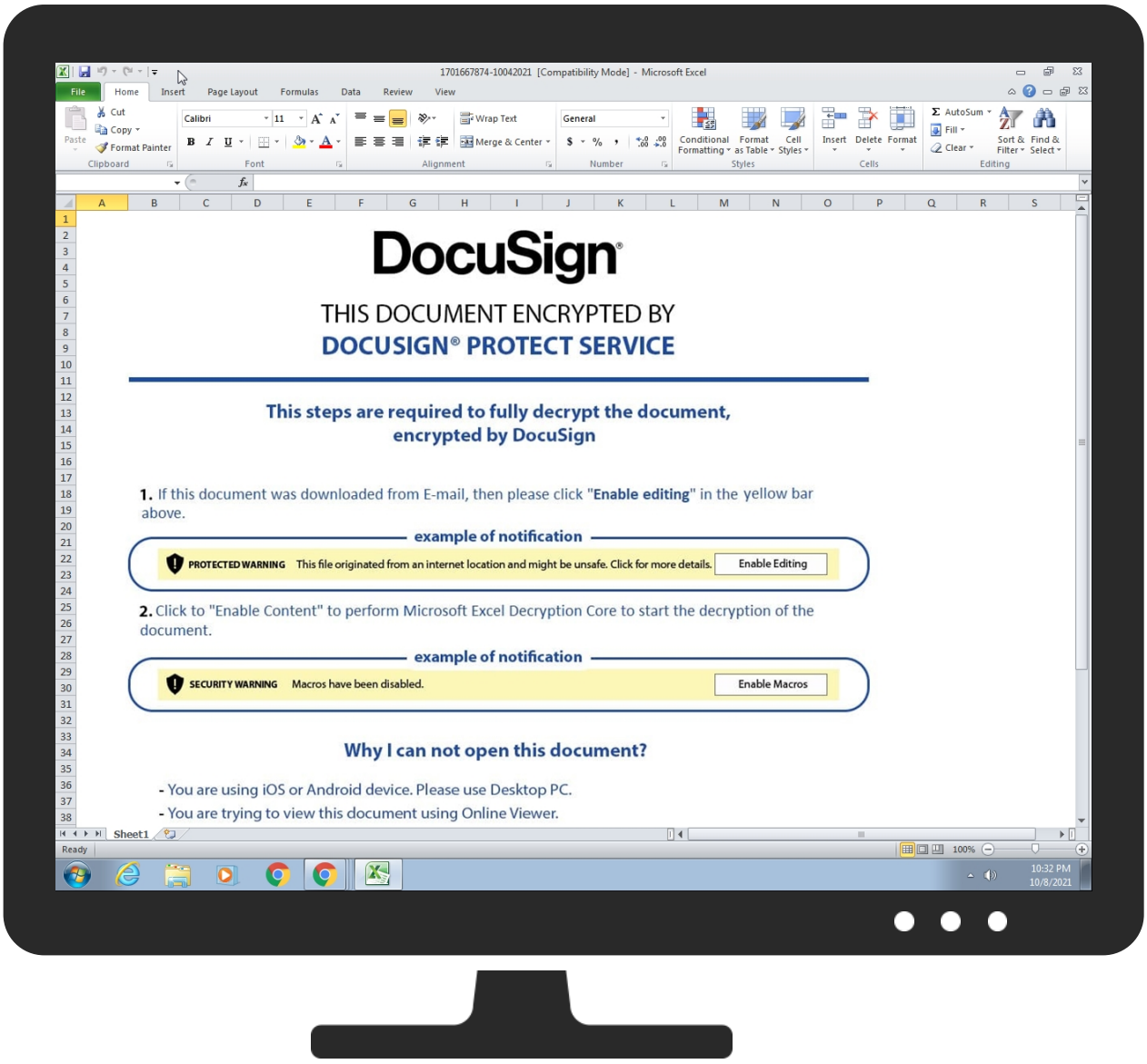


Screenshots

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://190.14.37.165/	4%	Virustotal		Browse
http://190.14.37.165/	0%	Avira URL Cloud	safe	
http://188.119.113.3/	4%	Virustotal		Browse
http://188.119.113.3/	0%	Avira URL Cloud	safe	
http://5.196.247.11/	4%	Virustotal		Browse

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://5.196.247.11/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	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
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:	22:30:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1701667874-10042021.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:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.expl.winXLS@7/2@0/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2021

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	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
	Document_143276485-Copy.xls	Get hash	malicious	Browse	• 193.38.54.149

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	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
	MT103-384849392983.doc	Get hash	malicious	Browse	• 158.69.91.158
OffshoreRacksSAPA	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
	Compensation-1214892625-09272021.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\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254323210253177
Encrypted:	false
SSDEEP:	1536:C6aL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CbJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	CB869BE78123435D1424E8D46E109C0B

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
SHA1:	5F7F80EB1C733006623828551737BBB312563659
SHA-256:	3CBA343B556B4D7DD4331CB01FC4DD64992C53998D0A0FE392A9B53DEE015297
SHA-512:	3E8DD0FB16306A8507352DCC97744C5C5E3A2A7C9C894888F84CC715C9CE5045787E04F5398BA84C7096B64BB795267DF11FF60FC433398C6D687A27D7165C3
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..... $.....x..xG.....T..... ....&!..... .....

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	15676
Entropy (8bit):	4.532584445930937
Encrypted:	false
SSDEEP:	192:RllA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:RL8xesT20lheZ3waE5D7qxIxkxe
MD5:	76E42ECC749A94DE9640F3AB385B214E
SHA1:	ED8C80ACAA1AA06590770D3854B2BDF248AD6F15
SHA-256:	469812A4111C69521D0F8CF6103F9087F5EBE4D8976948C8E330622944A30D4E
SHA-512:	DB1BD45F231CAFFCC9FE75F5F955907CE0240C3777575DD48856E90D2D2024558690A1818BB33AE2FE4F1798535D73937547A68E6ECD05DF6B17C29D14CC822
Malicious:	false
Reputation:	low
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x.....x. .....$".....P.....$".....0....P..,..... ....0.....%".....H..."..... .....H.....(.....@.....P.....0.....`.....p...X... ..... .....W.!]iI..[S.0.t.....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:	e4eea286a4b4bcb4

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

Copyright Joe Security LLC 2021

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2016 Parent PID: 596

General

Start time:	22:30:16
Start date:	08/10/2021
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:	0x13fcb0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 2184 Parent PID: 2016

General

Start time:	22:32:26

Start date:	08/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac
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: 1612 Parent PID: 2016

General

Start time:	22:32:26
Start date:	08/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac1
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: 2528 Parent PID: 2016

General

Start time:	22:32:26
Start date:	08/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac2
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021