ID: 438634
Sample Name: idea-22543577.xlsm
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:16:20
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

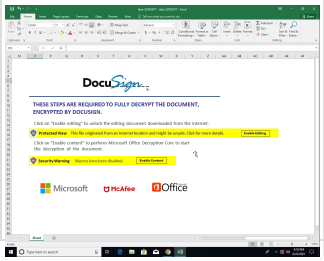
Windows Analysis Report idea-22543577.xlsm

Overview

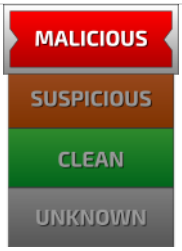
General Information

Sample Name:	idea-22543577.xlsm
Analysis ID:	438634
MD5:	690a255b0f1b59b.
SHA1:	1036eaadc0201b..
SHA256:	2aba85eff52ce4b..
Infos:	

Most interesting Screenshot:



Detection



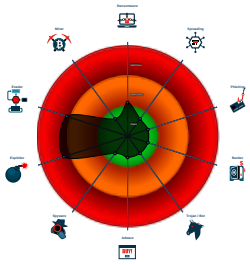
Hidden Macro 4.0

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Excel documents contains an embe…
- Found a high number of Window / Us…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6740 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 6916 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - regsvr32.exe (PID: 960 cmdline: regsvr32 ..\wail1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6340 cmdline: regsvr32 ..\wail2.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

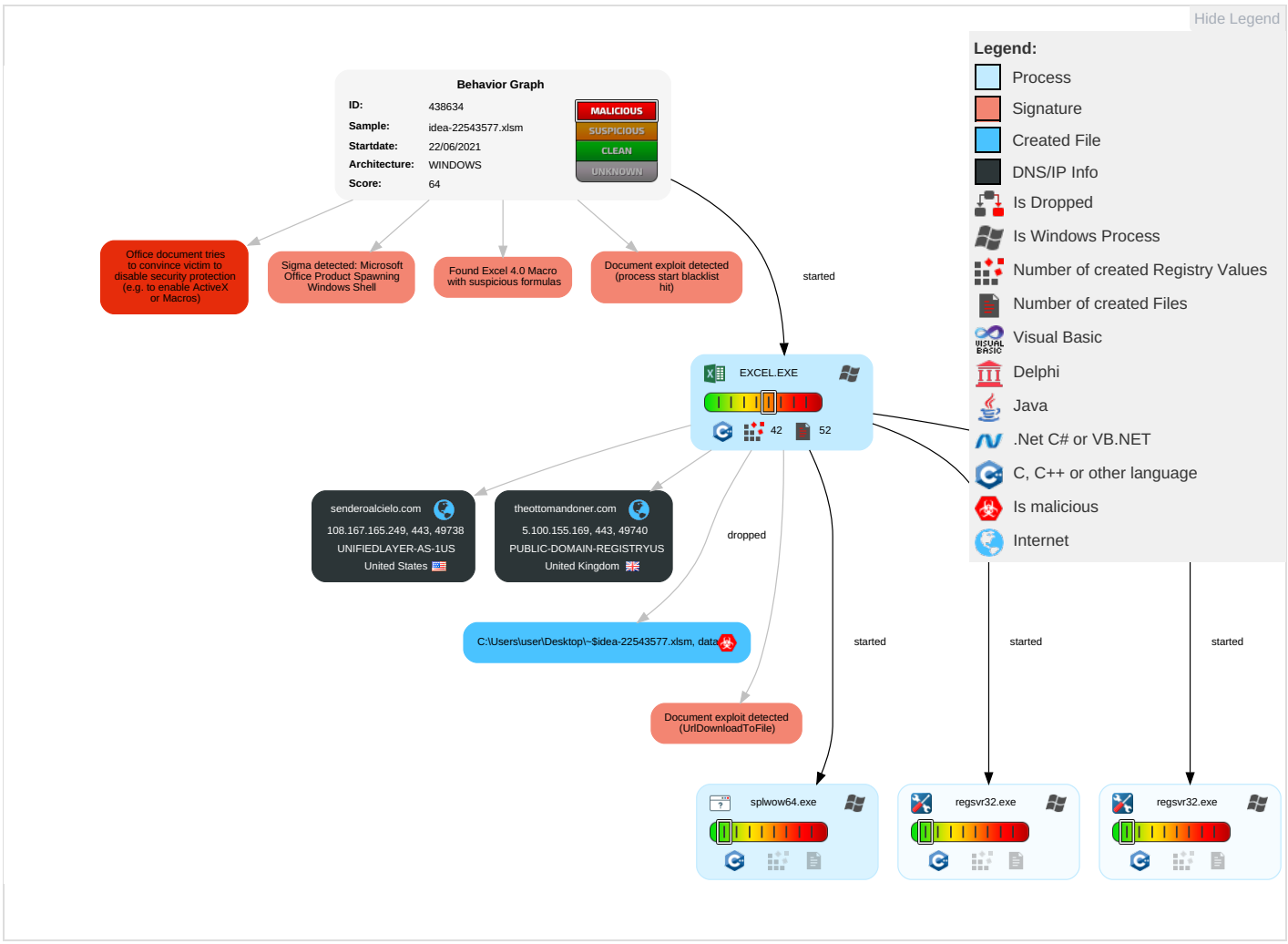
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatior
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

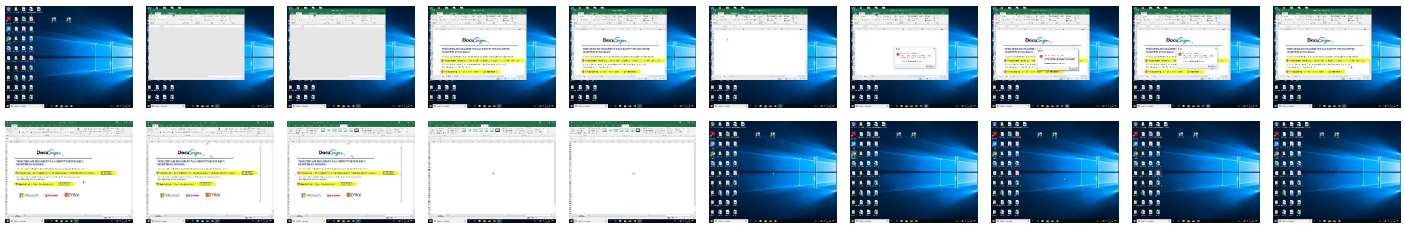
Behavior Graph

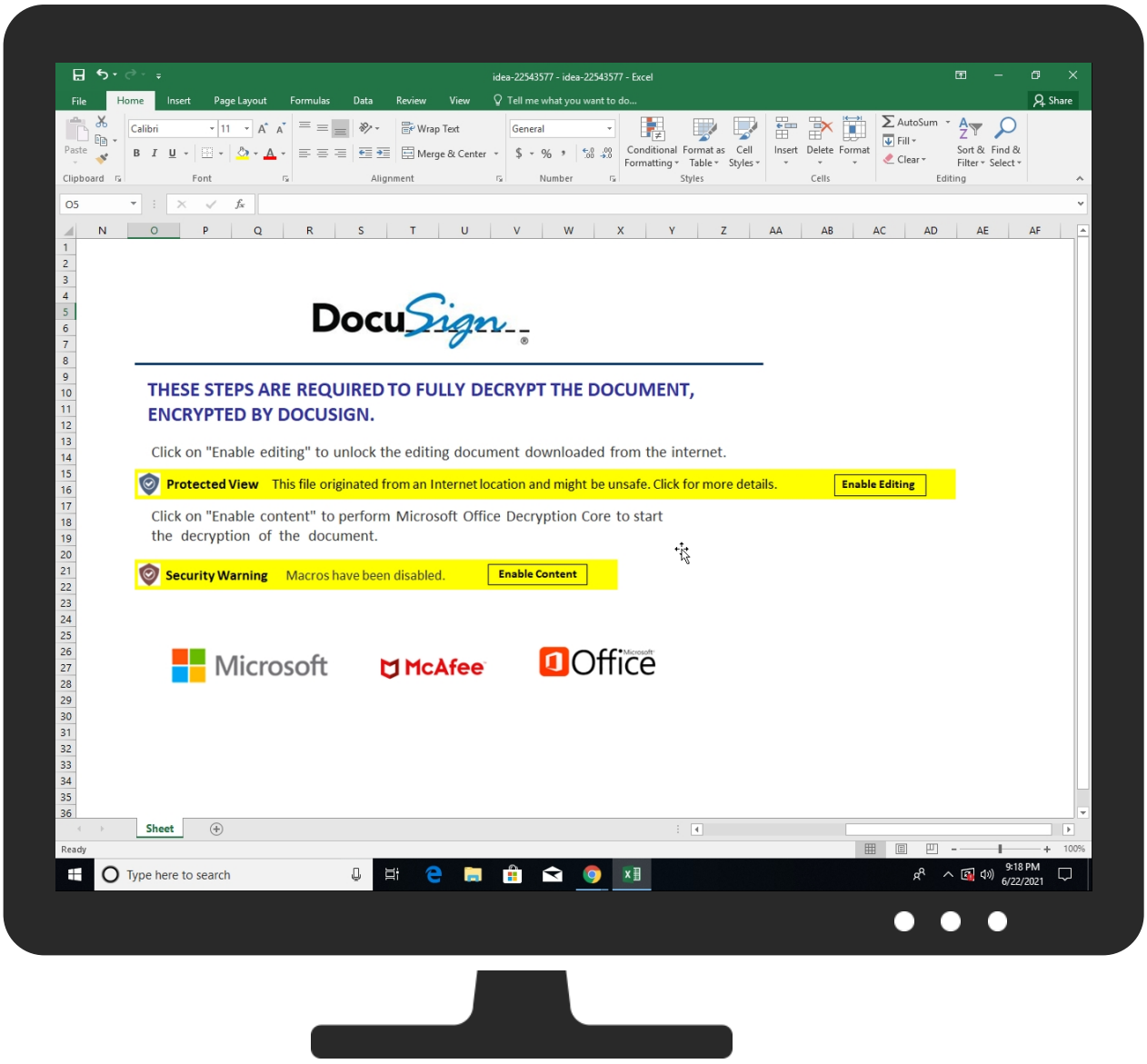


Screenshots

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
theottomandoner.com	2%	Virustotal		Browse
senderoalcielo.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	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://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	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://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	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://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.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://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	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://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	
http://https://staging.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theottomandoner.com	5.100.155.169	true	false	• 2%, Virustotal, Browse	unknown
senderoalcielo.com	108.167.165.249	true	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.100.155.169	theottomandoner.com	United Kingdom		394695	PUBLIC-DOMAIN-REGISTRYUS	false
108.167.165.249	senderoalcielo.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438634
Start date:	22.06.2021
Start time:	21:16:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s

Copyright Joe Security LLC 2021

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	idea-22543577.xlsm
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:	mal64.expl.evad.winXLSM@7/9@2/2
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: .xlsm • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
21:17:14	API Interceptor	1143x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
5.100.155.169	http://y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f6261636e636f2e7074	Get hash	malicious	Browse	• y.novobanco.opengateautospray.com/674616e69612e726f7361406e6f766f6261636e636f2e7074
108.167.165.249	idea-22543577.xlsm	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
senderoalcielo.com	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249
	Fra8994.exe	Get hash	malicious	Browse	• 162.241.60.126
	WXs8v9QuE7.exe	Get hash	malicious	Browse	• 50.87.146.99
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 192.185.88.195
	Order.exe	Get hash	malicious	Browse	• 108.167.183.94
	Habib_Bank Payment Advice.doc__.rtf	Get hash	malicious	Browse	• 162.144.79.7
	heoN5wnP2d.exe	Get hash	malicious	Browse	• 74.220.199.8
	FidKy67SWO.exe	Get hash	malicious	Browse	• 192.254.185.252
	RFQ-BCM 03122020.exe	Get hash	malicious	Browse	• 50.87.249.240
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 192.185.21.116
	idea-1232922316.xlsb	Get hash	malicious	Browse	• 162.241.194.107
	Orden de compra.exe	Get hash	malicious	Browse	• 192.185.0.218
	Drawing.exe	Get hash	malicious	Browse	• 162.241.61.229
	aim-1028486377.xlsb	Get hash	malicious	Browse	• 192.232.222.161
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 162.214.148.174
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.61.218
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 162.241.87.244
	eHTLcWfhgv.exe	Get hash	malicious	Browse	• 74.220.199.8
PUBLIC-DOMAIN-REGISTRYUS	idea-22543577.xlsm	Get hash	malicious	Browse	• 5.100.155.169
	Fra8995.exe	Get hash	malicious	Browse	• 208.91.198.143
	Fra8996.exe	Get hash	malicious	Browse	• 208.91.198.143
	Fra8997.exe	Get hash	malicious	Browse	• 208.91.199.223
	plan-1637276620.xlsm	Get hash	malicious	Browse	• 103.50.160.62
	aim-1028486377.xlsb	Get hash	malicious	Browse	• 103.21.59.25
	7qVSiXSTdETO7cX.exe	Get hash	malicious	Browse	• 208.91.198.143
	PI Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	Payment Advice Note from 21.06.2021 to 608720.exe	Get hash	malicious	Browse	• 208.91.199.225
	Inquiry pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	HYr6YeH1RP.exe	Get hash	malicious	Browse	• 208.91.198.143
	fng1AXSgue.exe	Get hash	malicious	Browse	• 208.91.199.225
	memorandum.exe	Get hash	malicious	Browse	• 208.91.199.223
	Bank Betails.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.854.8381.exe	Get hash	malicious	Browse	• 208.91.199.233
	AWB & Shipping Documents.exe	Get hash	malicious	Browse	• 208.91.199.224
	order no ORD00404083_01.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO#4500484210.exe	Get hash	malicious	Browse	• 208.91.199.233
	Request for Catalog and quotation.exe	Get hash	malicious	Browse	• 208.91.198.143
	INQUIRY pdf.exe	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	OzygoxrbzzvtmyjupcpndcovpjxtqpiywjSigned.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	2t71031BUz.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	DmtxjmmsiwawliehhrzxcpwdxtexpegwgoSigned.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249
	3yBar59k6g.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.165.249

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rVkZUqVZ40.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	idea-1232922316.xlsb	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	askinstall41.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	askinstall41.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	Potvrda o uplati u eurima.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	6Lld5WlJBW.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	pvWf7hYnWu.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	TT_COPY.MT103.SWIFT.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	MT103.docx	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	FAX.HTML	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	VM_5823_05_24_2-2.html	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	Outside Caller 06-18-21.HTML	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	KTOpmUzBlp.xls	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249
	MzhINp1fRi.exe	Get hash	malicious	Browse	• 5.100.155.169 • 108.167.16 5.249

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FF586352-751C-4478-9E87-FF9CF397D4DE	
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):	134914
Entropy (8bit):	5.367825535284073
Encrypted:	false
SSDEEP:	1536:pcQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:xEQ9DQW+zvXO1
MD5:	07158A29A2EEE64999158D2BE14B8807
SHA1:	65917A4FB5D0653E2419414FB22C5C0B7E1C9588
SHA-256:	DF7E37BE4E59DE60F520C6FBF06319843BC5A6CF96A8FBFC74B51740117DB4A4
SHA-512:	7E6951CC1EFE2F72958F07F4F6DC35D6C94578176C4E677FA4A5AA6DC8048F06744CC1B45ED4F656E64112261D2665DD0C4394BDD1980C3719735F02F4F82125
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="2021-06-22T19:17:14">.. Build: 16.0.14221.30525-->.. <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:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\12BD43E5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1133 x 589, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	75711
Entropy (8bit):	7.915372969602997
Encrypted:	false
SSDEEP:	1536:gxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncT:7br0o45GUgHhX8jC9yST
MD5:	8296338A43942E3107802E3062AC1270
SHA1:	46E67A586ED8A961AF7FD03140547C1CB2BAC227
SHA-256:	BE5F61F2AE8E4C9F9ADBCE5EC33D4C01A331734FFC5818AA8E45CF60456C5ABD
SHA-512:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171A D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...m...M.....p.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....g.....q.|.....<...'r....-^..c.If..ffX1K.[....Z....V.LO5L..J+...z.]]u..>.==.....Q..... (.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....j.7ZP...:...0S....z5T.....).WU =j.*.$H.B.P.)l.6Q..'.l..7..k..J.o..._....6..{C...r.\|2W.[a...m.BI.?...5.....D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._.,..I.\|a.7+>.....A#.....3v..37.....w(..j.. .C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...I5.e.b...V..\|..d../.....vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.....#!...T...C.#.>.E,[.,.....E....h~B.Y./....(2.....(...`....~w#.% ..R..{.....N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q..''...W2.....Q...G...z....Ea.....

C:\Users\user\AppData\Local\Temp\9DC40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	93025
Entropy (8bit):	7.835909433031108
Encrypted:	false
SSDEEP:	1536:TsxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncLHdVlz9:TXbr0o45GUgHhX8jC9ySLHBh
MD5:	3BDF2667F12D4D905D0DC4AFC01E4C63
SHA1:	9D26FEFA0B736F038570EFB98D8755B7D0930AE2
SHA-256:	2F2B4F6BBCE9B1246B9D99752EC70FAFDBBDFF8A8FC2020A758EB35C5109C0D3
SHA-512:	C5105394DCCD97D89839D4096019F7C84A5DC45E222D9D473E1AC740EE5F069C020D59D4C7EBA276C9CD3E047C2580FB83785DED1E0D2A638D91A84B615303
Malicious:	false
Reputation:	low
Preview:	.V.n.0....?.....r.Y.m...@.c.07p.....e.m.....m...q...jaM....w5;.F..'.....++0.....j..dW..O..e.,(.a...7.Q.`.V>.....V$z...B.E..|4.....)c....f...vA.WJ...z._.....h)....N.!).l.%(/.,AW."..-@...Q.c|.. (1d|.3.....Ys.>....~2{.*..R.V.<%..a.#.....ZAq/b.,.....8.z?.6.d3-...`.....S.4&.{U....D...v...H6._...S.....B.gv6e=.9.7....v...t..T...}.X./.Kw.....R.....p.....C...9..?...PQ.d...8...h. /5....R.....m*G... &..F5.....n.'..j..w'../.....PK.....!.!=J.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Tue Jun 22 18:17:21 2021, atime=Tue Jun 22 18:17:21 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.668812718446673
Encrypted:	false
SSDEEP:	12:8vXU/duCH2KOg4dc4L6f8+WrjAZ/DYbD+SeuSeL44t2Y+xIBjKZm:8QigmK2AZbcDg7aB6m
MD5:	AC114E5AF0816A9FFEBCDDF67409B7D1
SHA1:	19C55A294B5D04C4627FB777C450A4DA8BF5882C
SHA-256:	8229291C89D45BBD3B32FB1688BEA4444CC78C78710389D3C6FB6BA37C85AA55
SHA-512:	0D49F48BD71D73BDF63C96922856548A886868D0177C246D1433BF7161C765966600DDB798E385DB99B6CD7F795D18EDA323B392756D2E839D23362EDDD62000
Malicious:	false
Reputation:	low
Preview:	L.....F.....-..8..9.g.....9.g...0.....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.....#J.....T..j.o.n.e.s.....~.1.....R+...Desktop.h.....N...R+.....Y.....>.....p.).D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\....\....\....\....\.D.e.s.k.t.o.p.....:.,.LB.)...As..`.....X.....651689.....!a..%.H.VZAj...m<..... .....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9 ...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\idea-22543577.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:52 2020, mtime=Tue Jun 22 18:17:22 2021, atime=Tue Jun 22 18:17:22 2021, length=93025, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\idea-22543577.LNK	
Size (bytes):	2150
Entropy (8bit):	4.7168949323016856
Encrypted:	false
SSDEEP:	24:8ht7igmnAkCY5nhACbUjQnjD47aB6myht7igmnAkCY5nhACbUjQnjD47aB6m:877ixJnyCiQnlB6p77ixJnyCiQnlB6
MD5:	5F23734177853EFE4B1E30E48651F5B1
SHA1:	0CCCD5FB9265BFEF5BCDA0FC255263D48ACD433F
SHA-256:	629DB93CCB986DC37646B5DACCAD835A2F8DA5E4789B30FA0EE0A7D46199AB23
SHA-512:	99B2A76C403EFCD034EA5A9300061346AED94DDED7F28FEF396CC3AD9091B1F8F1C2490994F8D05594011752BBD9C7FF5F8105CF7467521108F74759217D90CA
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....CS.....f.9.g...f.9.g..ak.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...R.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.....N...R.....#J.....T..j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N...R.....Y.....>.....lN.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....r.2..l...R$. .IDEA-2~1.XLS..V.....>Q{<.R$.....V...../...i.d.e.a.-.2.2.5.4.3.5.7.7...x.l.s.m.....X.....-.....W.....>.S.....C:\Users\user\Desktop\idea-22543577.xlsm..).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.i.d.e.a.-.2.2.5.4.3.5.7.7...x.l.s.m.....:.,.LB.)...As...`.....X.....651689.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	94
Entropy (8bit):	4.621739484560059
Encrypted:	false
SSDEEP:	3:oyBVomxWHzXdUlUBhXXdUlmxWHzXdUlv:dj07bxy7E
MD5:	E7873154CD23EE19AAA8800DC776A9B5
SHA1:	BB75A07FBBC9BE7C5F38BB058ED8198336C4F73C
SHA-256:	6E67DB062BE87713F064EF905334EB421CC07ABB115DD7975323EF1EDBAD4F13
SHA-512:	8844B76DFF4AF8A235E5B791ADD65A951FEF222C64450AC98D2F3C94F7B08791A1DC64F5DFECC90EE228EF82BB0D0918E6AE77E9E836D8541FD0F4934026D45C
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[misc]..idea-22543577.LNK=0..idea-22543577.LNK=0..[misc]..idea-22543577.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\9EC40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	93025
Entropy (8bit):	7.835909433031108
Encrypted:	false
SSDEEP:	1536:TsxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncLHdVlz9:TXbr0o45GUgHhX8jC9ySLHBh
MD5:	3BDF2667F12D4D905D0DC4AFC01E4C63
SHA1:	9D26FEFA0B736F038570EFB98D8755B7D0930AE2
SHA-256:	2F2B4F6BBCE9B1246B9D99752EC70FAFDBBDFF8A8FC2020A758EB35C5109C0D3
SHA-512:	C5105394DCCD97D89839D4096019F7C84A5DC45E222D9D473E1AC740EE5F069C020D59D4C7EBA276C9CD3E047C2580FB83785DED1E0D2A638D91A84B615303
Malicious:	false

C:\Users\user\Desktop\9EC40000	
Preview:	.V.n.0....?.....r.Y.m...@.c.07p.....e.m.....m...q...jaM....w5;.F..'.....++0.....j..dW..O..e.,(.a...7.Q.`.V>.....V$z...B.E..|4.....)c....f...vA.WJ...z._.....h)....N.!).I.%(/..AW."..-@...Q.c|..(1d|.3.....Ys.>....~2{.*..R.V.<%..a.#.....ZAq/b..,.....8.z?.6.d3-...`.....S.4&.{U....D...v...H6._...S.....B.gv6e=.9.7....v...t..T...}.X./.Kw.....R.....p.....C...9..?...PQ.d...8...h./5....R.....m*G... &..F5.....n.'..j..w'../.....PK.....!.!=J.....[Content_Types].xml ...(..... ....

C:\Users\user\Desktop\~$idea-22543577.xlsm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtBhFXI6dtt:RJZhJ1
MD5:	836727206447D2C6B98C973E058460C9
SHA1:	D83351CF6DE78FEDE0142DE5434F9217C4F285D2
SHA-256:	D9BECB14EECC877F0FA39B6B6F856365CADF730B64E7FA2163965D181CC5EB41
SHA-512:	7F843EDD7DC6230BF0E05BF988D25AE6188F8B22808F2C990A1E8039C0CECC25D1D101E0FDD952722FEAD538F7C7C14EEF9FD7F4B31036C3E7F79DE570CD06 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . . ..pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.835191332560826
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	idea-22543577.xlsm
File size:	93205
MD5:	690a255b0f1b59b3421800bab8b41c10
SHA1:	1036eaadc0201b50d3d005ad05e208888021b945
SHA256:	2aba85eff52ce4b7d41b651baec98fea810a3307dc2b90bebf1c68131018cb0f
SHA512:	a124c5e4e8cdacc52e84ab89e92f83cbf535b3757271fde02bdb8b9b254c10f1bc2a05e09ed2dc9f3b1f605f698da6970048ea4fc187375c860b745cb551f8d1
SSDEEP:	1536:CaxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncEya2/dLBT0y:Clbr0o45GUgHhX8jC9ySXDLB/
File Content Preview:	PK.....!.!=J.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74ecd0e2f696908c

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "idea-22543577.xlsm"

Indicators

Has Summary Info:	
Application Name:	

Indicators

Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

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
Jun 22, 2021 21:17:24.075067043 CEST	192.168.2.4	8.8.8.8	0xc58e	Standard query (0)	senderoalcielo.com	A (IP address)	IN (0x0001)
Jun 22, 2021 21:17:26.222008944 CEST	192.168.2.4	8.8.8.8	0x6d7f	Standard query (0)	theottomandoner.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 22, 2021 21:17:24.134171009 CEST	8.8.8.8	192.168.2.4	0xc58e	No error (0)	senderoalcielo.com		108.167.165.249	A (IP address)	IN (0x0001)
Jun 22, 2021 21:17:26.281980038 CEST	8.8.8.8	192.168.2.4	0x6d7f	No error (0)	theottomandoner.com		5.100.155.169	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 21:17:24.474009037 CEST	108.167.165.249	443	192.168.2.4	49738	CN=senderoalcielo.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun May 30 04:16:52 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sat Aug 28 04:16:52 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 22, 2021 21:17:26.400989056 CEST	5.100.155.169	443	192.168.2.4	49740	CN=www.theottomandoner.theottomandoner.co.uk CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Jun 21 15:18:17 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Sep 19 15:18:16 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6740 Parent PID: 800

General

Start time:	21:17:11
Start date:	22/06/2021
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:	0xa40000
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: splwow64.exe PID: 6916 Parent PID: 6740

General

Start time:	21:17:14
Start date:	22/06/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff77ee90000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
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: 960 Parent PID: 6740

General

Start time:	21:17:26
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\wail1.dll
Imagebase:	0x1040000
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: 6340 Parent PID: 6740

General

Start time:	21:17:26
Start date:	22/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	regsvr32 ..\wail2.dll
Imagebase:	0x1040000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021