

ID: 441941
Sample Name: diagram-1878769052.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:27:06
Date: 29/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report diagram-1878769052.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
Signature Overview 5
AV Detection: 5
Software Vulnerabilities: 5
Networking: 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 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 14
General 14
File Icon 14
Static OLE Info 14
General 14
OLE File "diagram-1878769052.xls" 14
Indicators 14
Summary 14
Document Summary 15
Streams 15
Macro 4.0 Code 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTPS Packets 15
Code Manipulations 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: EXCEL.EXE PID: 7076 Parent PID: 800 16
General 16
File Activities 16
File Created 16
File Deleted 16
Registry Activities 16
Key Created 16
Key Value Created 16
Analysis Process: rundll32.exe PID: 1288 Parent PID: 7076 16

General 16
File Activities 17
Analysis Process: rundll32.exe PID: 1076 Parent PID: 7076 17
General 17
File Activities 17
Disassembly 17
Code Analysis 17

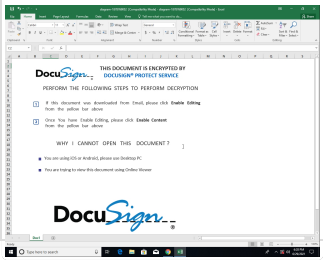
Windows Analysis Report diagram-1878769052.xls

Overview

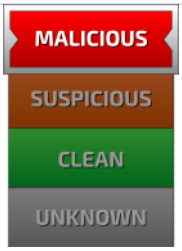
General Information

Sample Name:	diagram-1878769052.xls
Analysis ID:	441941
MD5:	5dc0dbb9a817db..
SHA1:	6e51ed7744080f5.
SHA256:	22c8c25451ead7..
Infos:	

Most interesting Screenshot:



Detection



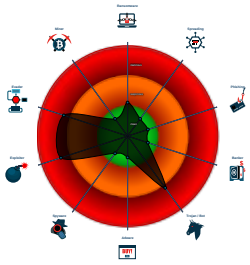
Hidden Macro 4.0

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …
- Outdated Microsoft Office dropper d…
- Sigma detected: Microsoft Office Pr…
- Yara detected hidden Macro 4.0 in E…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7076 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 1288 cmdline: rundll32 ..\durio.fur,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 1076 cmdline: rundll32 ..\durio.fur1,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
diagram-1878769052.xls	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	
diagram-1878769052.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

Copyright Joe Security LLC 2021

Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:



Outdated Microsoft Office dropper detected

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

Found abnormal large hidden Excel 4.0 Macro sheet

HIPS / PFW / Operating System Protection Evasion:

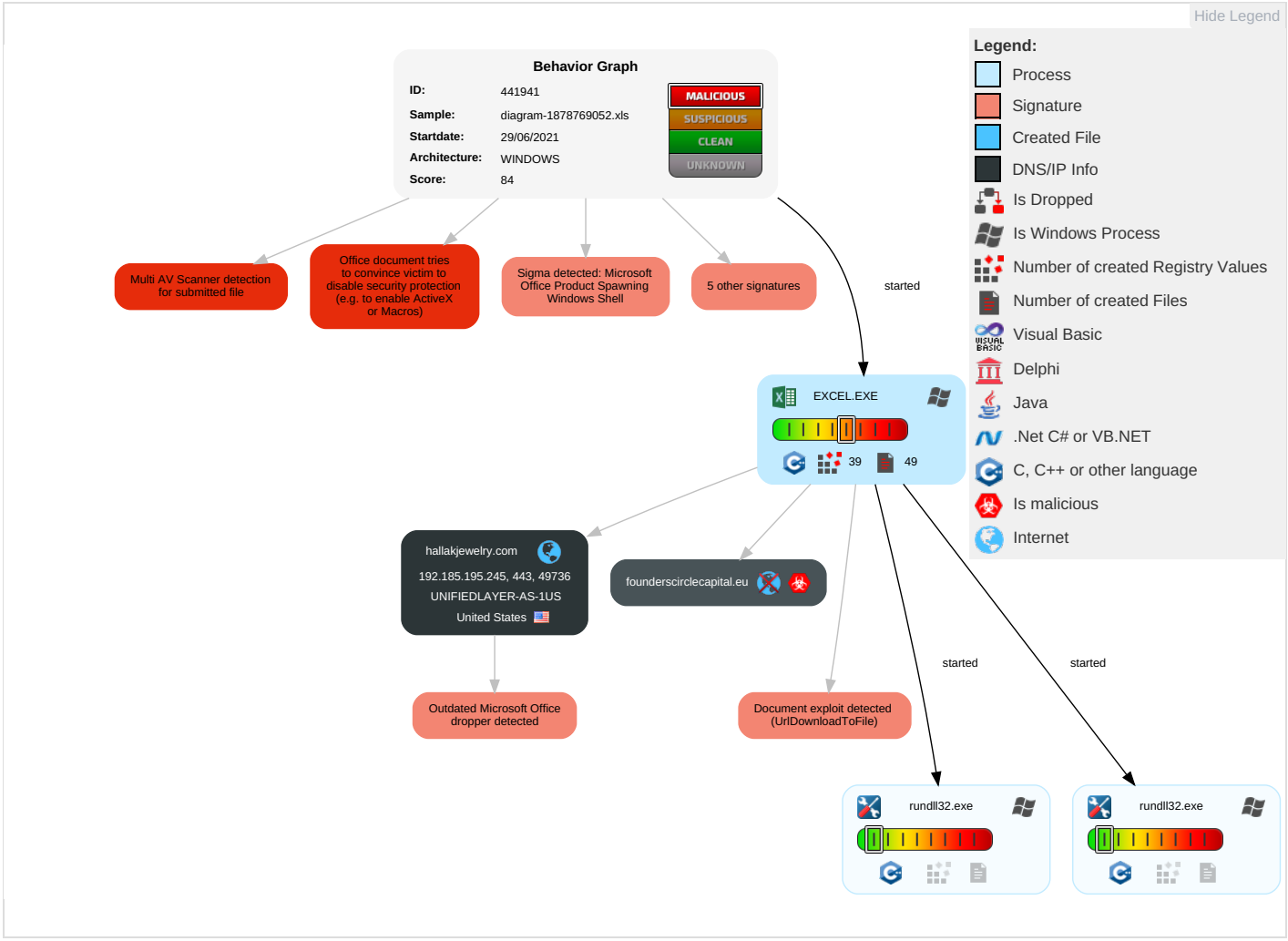


Yara detected hidden Macro 4.0 in Excel

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 2	Path Interception	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 Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

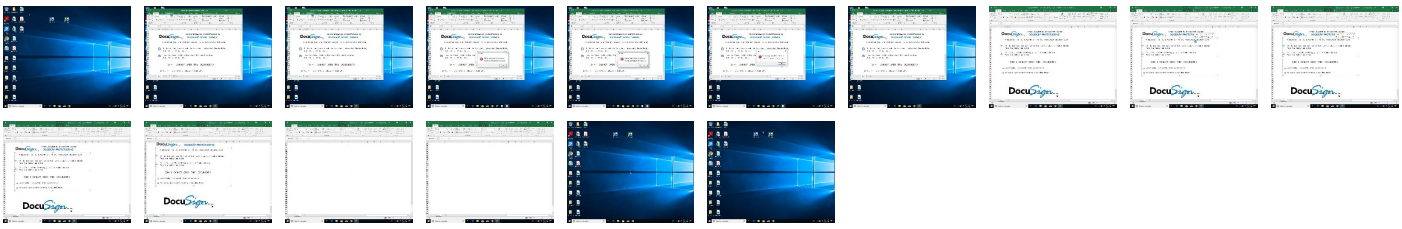
Behavior Graph

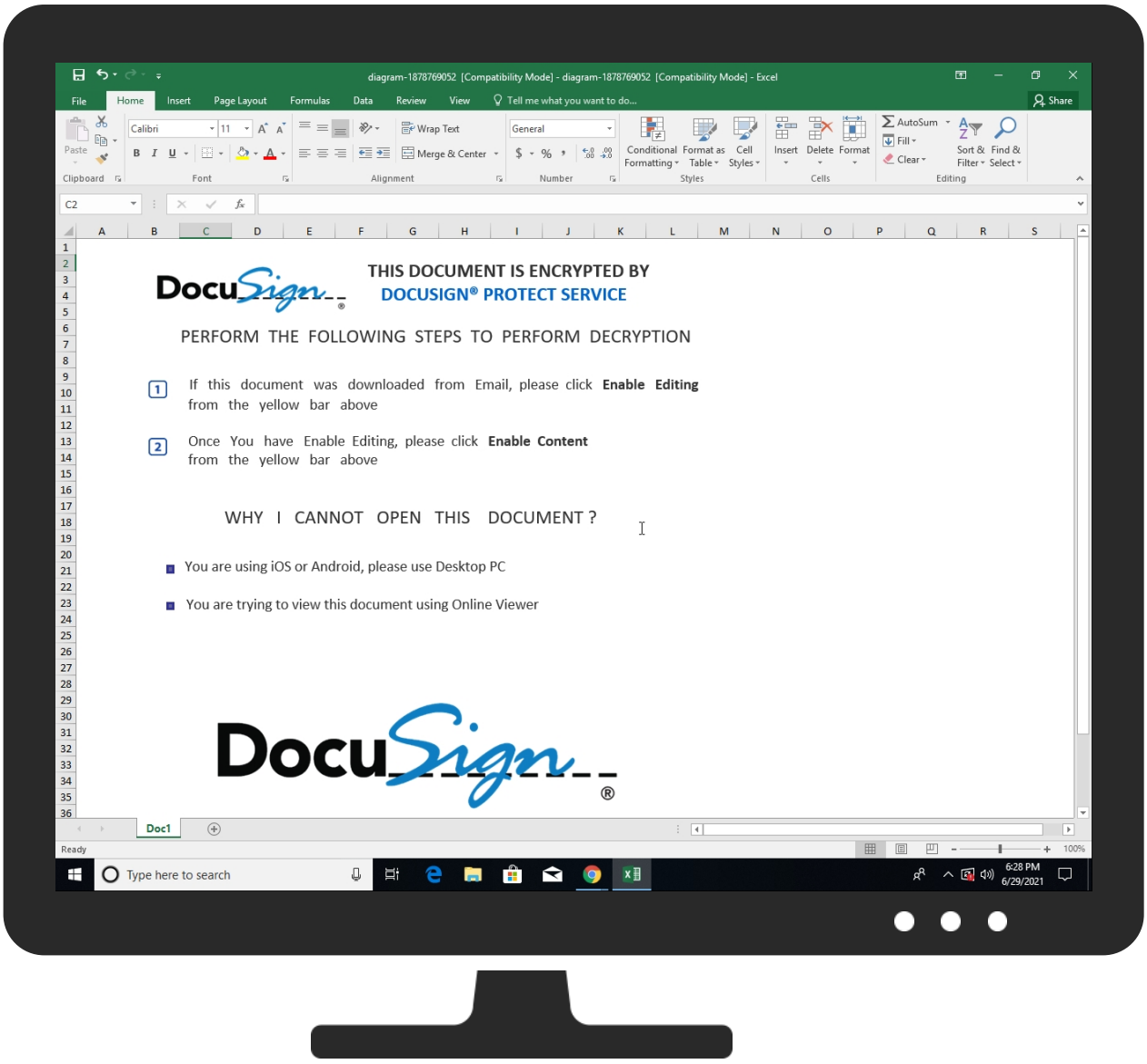


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
diagram-1878769052.xls	38%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

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://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://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://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://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%	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.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://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://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://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	
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	

Source	Detection	Scanner	Label	Link
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
hallakjewelry.com	192.185.195.245	true	false		unknown
founderscirclecapital.eu	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.195.245	hallakjewelry.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	441941
Start date:	29.06.2021
Start time:	18:27:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	diagram-1878769052.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:	18
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:	mal84.troj.expl.evad.winXLS@5/7@2/1
EGA Information:	Failed
HDC Information:	Failed

Copyright Joe Security LLC 2021

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
192.185.195.245	diagram-1878769052.xls	Get hash	malicious	Browse	
	diagram-586589391.xls	Get hash	malicious	Browse	
	diagram-586589391.xls	Get hash	malicious	Browse	
	diagram-816901094.xls	Get hash	malicious	Browse	
	diagram-816901094.xls	Get hash	malicious	Browse	
	diagram-90301250.xls	Get hash	malicious	Browse	
	diagram-90301250.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hallakjewelry.com	diagram-586589391.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-586589391.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-816901094.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-816901094.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-90301250.xls	Get hash	malicious	Browse	• 192.185.195.245
	diagram-90301250.xls	Get hash	malicious	Browse	• 192.185.195.245

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	diagram-1878769052.xls	Get hash	malicious	Browse	• 192.185.195.245
	statistic-1496367785.xls	Get hash	malicious	Browse	• 108.179.232.80
	statistic-1496367785.xls	Get hash	malicious	Browse	• 108.179.232.80
	4dvYb6Nq3y.exe	Get hash	malicious	Browse	• 50.87.238.189
	Remittance.xls	Get hash	malicious	Browse	• 162.241.120.180
	SecuriteInfo.com.Trojan.Win32.Save.a.27842.exe	Get hash	malicious	Browse	• 192.185.164.148
	SEOCHANG INDUSTRY Co., Ltd..exe	Get hash	malicious	Browse	• 162.241.24.206
	7R9igRpuL4.msi	Get hash	malicious	Browse	• 192.185.0.218
	nxinF8KuKS.exe	Get hash	malicious	Browse	• 192.185.16.56

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	242jQP4mQP.exe	Get hash	malicious	Browse	• 50.87.248.20
	Halkbank.exe	Get hash	malicious	Browse	• 192.185.0.218
	HBenKsn2R8.exe	Get hash	malicious	Browse	• 96.125.162.104
	DC Viet Nam Order list 6-25-21.exe	Get hash	malicious	Browse	• 162.144.0.158
	Minutes of Meeting 22062021.exe	Get hash	malicious	Browse	• 108.167.156.42
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	factura y factura de la v#U00eda a#U00e9rea.exe	Get hash	malicious	Browse	• 74.220.199.6
	T5gtQGRL8u.exe	Get hash	malicious	Browse	• 162.241.135.156
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	statistic-1496367785.xls	Get hash	malicious	Browse	• 192.185.195.245
	Bank_ details.exe	Get hash	malicious	Browse	• 192.185.195.245
	prijenos SWIFT za partiju 220000000001182910.exe	Get hash	malicious	Browse	• 192.185.195.245
	PO29012021,pdf.ppam	Get hash	malicious	Browse	• 192.185.195.245
	OFfcxY5xia.exe	Get hash	malicious	Browse	• 192.185.195.245
	k72fFnCoEX.exe	Get hash	malicious	Browse	• 192.185.195.245
	DWJn18MuX6.exe	Get hash	malicious	Browse	• 192.185.195.245
	sp7UUM849P.exe	Get hash	malicious	Browse	• 192.185.195.245
	CL2SJ8-LYGF7Z-SEJ2QPPAPL.htm	Get hash	malicious	Browse	• 192.185.195.245
	AqZrR9upiM.exe	Get hash	malicious	Browse	• 192.185.195.245
	iduD2A1.dll	Get hash	malicious	Browse	• 192.185.195.245
	E6973qZ1cV.exe	Get hash	malicious	Browse	• 192.185.195.245
	97FC461FD24104740310BD741F7F8EBF489E640AA93A0.exe	Get hash	malicious	Browse	• 192.185.195.245
	Tu33yM3ZKj.exe	Get hash	malicious	Browse	• 192.185.195.245
	BNK1135000001.docx	Get hash	malicious	Browse	• 192.185.195.245
	message_zdm.html	Get hash	malicious	Browse	• 192.185.195.245
	Financial Statements.html	Get hash	malicious	Browse	• 192.185.195.245
	Wilson-McShane Corporation ACH.xlsx	Get hash	malicious	Browse	• 192.185.195.245
	Dfdvfczl_Signed_.exe	Get hash	malicious	Browse	• 192.185.195.245
	9irkb5Rbn8.exe	Get hash	malicious	Browse	• 192.185.195.245

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3C836C47-4F20-4ACD-A373-FE45E87498F5

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Copyright Joe Security LLC 2021

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\3C836C47-4F20-4ACD-A373-FE45E87498F5	
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	135209
Entropy (8bit):	5.363063821175687
Encrypted:	false
SSDEEP:	1536:JcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:dEQ9DQW+zwXO1
MD5:	EC3B0743FC28C8E80BE8E85BF2D3B49C
SHA1:	F3AFD5D06F1EF83239F9DBCFEDAA3E82D7B971E6
SHA-256:	B10B974159F945692DE4245A74A92AF19FA6A588B9E61EA299420BCF92380197
SHA-512:	676C1D9EE522D1EB917319F66205142A751969C1A22C818195B9611230EB28EDD9BB221A8E490C4C3B1ECCC0A3A7A73E75AAEE38F16A310D9D2C0DEF16046A8 9
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="2021-06-29T16:28:00">.. Build: 16.0.14228.30525-->.. <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\D7B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	81728
Entropy (8bit):	7.903508224175571
Encrypted:	false
SSDEEP:	1536:bMCB8zQP16QCI/UyfqKdpkatlASfkuZHMqCVxI118t1oHN9IKb:bNP16QjJfVkZGp1Su18t1oHNN
MD5:	1AAE9170F9650321D1EDE8446ED69E62
SHA1:	FE08C76F03E1C4FFDD3142944A95996439EEC606
SHA-256:	9C884CD661FF266D2D2C3244046DB797D7A0AD74D06884FB7641B11D938F8458
SHA-512:	8F22DB18A506A3ADDCF32B02444EE20281E038C763E4BA0AB4ACA5608FE3AB72846B9C77D63A8DE642199FC0C3615B63C802D9DA96AE62BEB466E7F0148A51 D1
Malicious:	false
Reputation:	low
Preview:	.U.N.0.}G.....J\@Z!....w.`?....U..1..=c7..JK)...'s.3.x|...z.....7#V..^i....u}.*L.)a...-.....n..+.v.>.p.9.....p...hE.... .\t.OF._\z...:e.6._.L.T]-hy.d...~...T-.!.-E"....w$.....%..C....H.4!jb..... o...{.m..7gD0.....2K)..?...r.c.....T7".?.[|a.....f;H6.b....).5V.....Y.....?A.v.l._.....Qt.B....b.....c..t.....\..g..a'.....6..].k..:T..Y.....}...K3.&..4.#....D..u .I.z.m..kF.....@m...<.. .....PK.....!.[:.....[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 29 15:28:02 2021, atime=Tue Jun 29 15:28:02 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.664189479719172
Encrypted:	false
SSDEEP:	12:8JfXUM+lzjduCH2KOtd342scR+WrjAZ/DYbD9SeuSeL44t2Y+xIBjKZm:8J4zxitN3AZbcDz7aB6m
MD5:	A3D4465FB4FA6417CAD47967513FDDB4
SHA1:	087D7A064B3259FBB1EEAE8D3B0AD5D22B7FBB56
SHA-256:	0DE09FB970639B2273509C9D9355CEE562287A4C84DF222F4CFD32B272598DE2
SHA-512:	3029F2EB55F00990AE768BE27150531727BE97E203032996DF2ECD1E9D4E7C560B9D5DC00F706ED0897E75D7917F10D953CD38E59AB542A25B9E3EB66940E2F5
Malicious:	false
Reputation:	low
Preview:	L.....F.....-....MI..m....F..m... .....u....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rt.....:.....;..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...Rt.....#J.....Q...j.o.n.e.s.....~.1.....R....Desktop.h.....N...R.....Y.....>.....C..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.....992547.....!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\diagram-1878769052.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 29 15:28:02 2021, atime=Tue Jun 29 15:28:02 2021, length=174592, window=hide
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\diagram-1878769052.LNK	
Size (bytes):	2190
Entropy (8bit):	4.719930747057183
Encrypted:	false
SSDEEP:	48:8hitFFRQYWnxiBB6phitFFRQYWnxiBB6:8hitjRQ/cKhitjRQ/c
MD5:	C10AB27FC43830657A472B57F330E2D6
SHA1:	CF4231FFDE0BF42143EBCBAC87FA270E9CE8D91F
SHA-256:	48EE3D7BDF0A11D170E85231C42FE4DFE72BCAC3C1FDD1F56BFFBEB208A3AA92
SHA-512:	E74A1B3F2D7642FDF3167C3114E6164D8B57044AAC76224F9D3C9A244B72D2DE1453341BDF5BD28E84BCA88F9CC4E8C596E524FF4B1B84566D87ED538CF44F 6
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....{.S.....Y..m....Y..m.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L...Rt.....:.....;..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...Rt.....#J.....Q...j.o.n.e.s.....~.1.....>Q}<..Desktop.h.....N...Rt.....Y.....>.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.- 2.1.7.6.9.....z.2..,....R{. .DIAGRA~1.XLS..^.....>Q{<.R{.....V.....u...d.i.a.g.r.a.m.-.1.8.7.8.7.6.9.0.5.2...x.l.s.....\.....-.....[.....>.S.....C:\Users\user\Desk top\diagram-1878769052.xls..-.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.i.a.g.r.a.m.-.1.8.7.8.7.6.9.0.5.2...x.l.s.....:.,.LB.)...As...`.....X.....992547.....!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.

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):	107
Entropy (8bit):	4.851195869560029
Encrypted:	false
SSDEEP:	3:oyBVomMXCUUkQN6lZFdUkQN6lmMXCUUkQN6lv:dj6XCvkQS8kQ6XCvkQy
MD5:	027E2AFCDD06DD3DF9CC94970FC294A4
SHA1:	C1F15C35ADF3EA115CA99740EEF8927F35C05154
SHA-256:	94AC427E287B5A0C4A4017D90BAB2D66485AC0A211640CA0CDD0687CB087CC93
SHA-512:	4456E497CCAD37068DA4AB5C12F547B1D36B749823F48674466565B92E7C927B1F830574BD51691B66B84136097D413B916E038F5BF09C8D4FB70C2D3CDB954A
Malicious:	false
Reputation:	low
Preview:	Desktop.LNK=0..[xls]..diagram-1878769052.LNK=0..diagram-1878769052.LNK=0..[xls]..diagram-1878769052.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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\B8B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	209068
Entropy (8bit):	5.656573528870952
Encrypted:	false
SSDEEP:	3072:3rNbP1vQjFfVkdG2fQPGVTPduUzvWnb+quX/DXfXbwXdrNRPi:xP1mfVUNRwXRPi
MD5:	170E97A7A4712CC4CC25FFFAF8B6E789
SHA1:	CB6AE55413CBE249566E5DEC1A90598751909159
SHA-256:	E34B19A41C8DBC4253EA79D6FE7D4467E3174F59415FC18D6933189DA0C04BE7
SHA-512:	94E4EF01EDE4551399D1983C86151CC8FA229FD6D1FF595D50D98F9D7F766EB0C5A51739EF25A0B2EAA458D5CC3DB55EEC533CB4A0C0E00D76393EABA2924 F9
Malicious:	false

C:\Users\user\Desktop\B8B40000	
Reputation:	low
Preview:	........T8.....\.p....pratesh B.....a.....=.....=.....i..9..8.....X.@. .....".....1.....P..C.a.l.i.b.r.i.1.....P..A.r.i.a.l.1.....P..A.r.i.a.l.1.....P..A.r.i.a.l.1.....P..C.a.l.i.b.r.i.1...h...8.....P..C.a.m.b.r.i.a.1... ,...8.....P..A.r.i.a.l.1.....8.....P..A.r.i.a.l.1.....8.....P..A.r.i.a.l.1.....<.....P..A.r.i.a.l.1.....4.....P..A.r.i.a.l.1.....4.....P..A.r.i.a.l.1.....P..C.a.l.i.b.r.i.1..... A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....A.r.i.a.l.1.....>.....A.r.i.a.l.1.....?.....A.r.i.a.l.1..... A.r.i.a.l.1.....A.r.i.a.l.1.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Grog, Last Saved By: Grog, Name of Creating Application: Microsoft Excel, Create Time/Date: Sat Sep 16 01:00:00 2006, Last Saved Time/Date: Thu May 20 08:01:36 2021, Security: 0
Entropy (8bit):	2.078617301736935
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	diagram-1878769052.xls
File size:	535552
MD5:	5dc0dbb9a817db4a5f589f670c6b9241
SHA1:	6e51ed7744080f5583beb20fd7052e2fcbf7cd3a
SHA256:	22c8c25451ead7742914a869f775af6e8751907a83b46077b8439d03a9105c81
SHA512:	ee37b3b4c2ba204b542a091104bda6f1a0097a17e131a79edf48f7fe3941d36df248bfd0c2dcc4c7d075abdc82730668587fa68e739175d58c0b5e9688edb260
SSDEEP:	1536:pq35xFlHVRl1X/7fi18snt52U20kyti4kmhRd+s2tebLxtf7t69KRGF:pq35xFl1Rl1Pas+ilmhR4s2tQVtfgDF
File Content Preview:	.....>..... ....

File Icon



Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "diagram-1878769052.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:	False

Summary

Code Page:	1251
Author:	Grog
Last Saved By:	Grog

Summary

Create Time:	2006-09-16 00:00:00
Last Saved Time:	2021-05-20 07:01:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary

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

Streams

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 29, 2021 18:28:03.833156109 CEST	192.168.2.4	8.8.8.8	0xf998	Standard query (0)	hallakjewelry.com	A (IP address)	IN (0x0001)
Jun 29, 2021 18:28:04.576205015 CEST	192.168.2.4	8.8.8.8	0xa968	Standard query (0)	foundersci rclecapital.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 29, 2021 18:28:03.890970945 CEST	8.8.8.8	192.168.2.4	0xf998	No error (0)	hallakjewelry.com		192.185.195.245	A (IP address)	IN (0x0001)
Jun 29, 2021 18:28:04.644221067 CEST	8.8.8.8	192.168.2.4	0xa968	Name error (3)	foundersci rclecapital.eu	none	none	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 29, 2021 18:28:04.221026897 CEST	192.185.195.245	443	192.168.2.4	49736	CN=hallakjewelry.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.	Sat May 15 06:53:35 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Fri Aug 13 06:53:35 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		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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: 7076 Parent PID: 800

General

Start time:	18:27:57
Start date:	29/06/2021
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:	0x8d0000
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: rundll32.exe PID: 1288 Parent PID: 7076

General

Start time:	18:28:03

Start date:	29/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\durio.fur,DllRegisterServer
Imagebase:	0x930000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 1076 Parent PID: 7076

General

Start time:	18:28:04
Start date:	29/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32 ..\durio.fur1,DllRegisterServer
Imagebase:	0x930000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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 Joe Sandbox Cloud Basic 32.0.0 Black Diamond