ID: 439554
Sample Name: plan-930205822.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 07:07:18
Date: 24/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

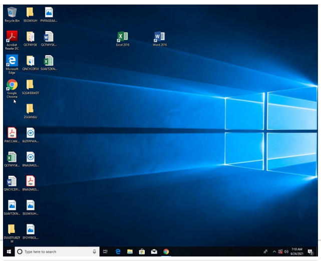
Windows Analysis Report plan-930205822.xlsb

Overview

General Information

Sample Name:	plan-930205822.xlsb
Analysis ID:	439554
MD5:	a9632052eafc78e.
SHA1:	2bade21221f175c.
SHA256:	ae39ed7fd03aae6.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

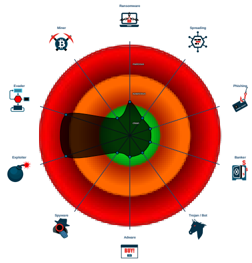
Hidden Macro 4.0

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

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- 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 …
- Sigma detected: Microsoft Office Pr…
- 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: 5716 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 4220 cmdline: regsvr32 ..\gihi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 1956 cmdline: regsvr32 ..\gihi2.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

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

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)

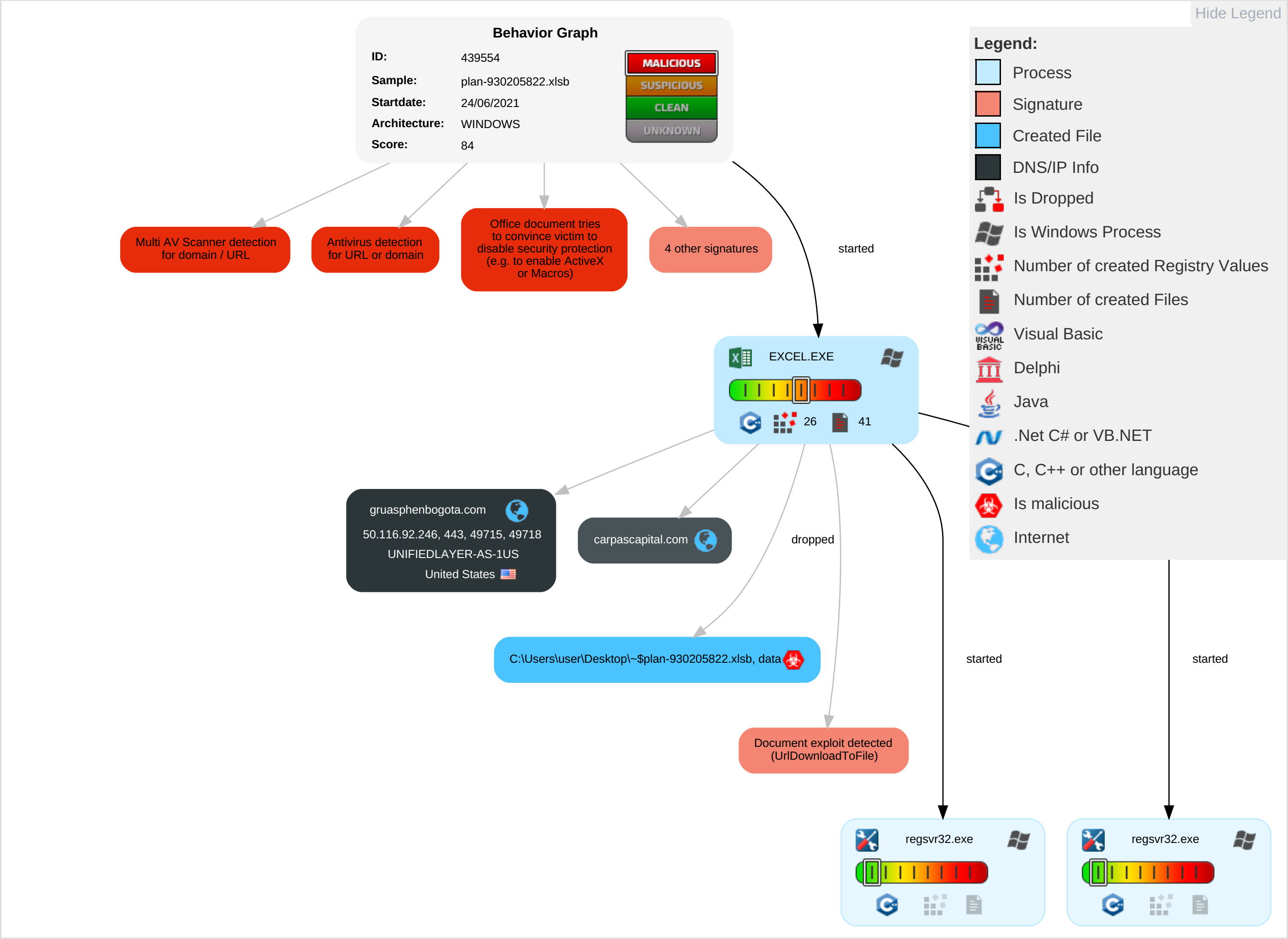
Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

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
Valid Accounts	Scripting 2	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 Communication	Remotely Track Devic Without Authorizatio
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	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 Authorizatio
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Regsvr32 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 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	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

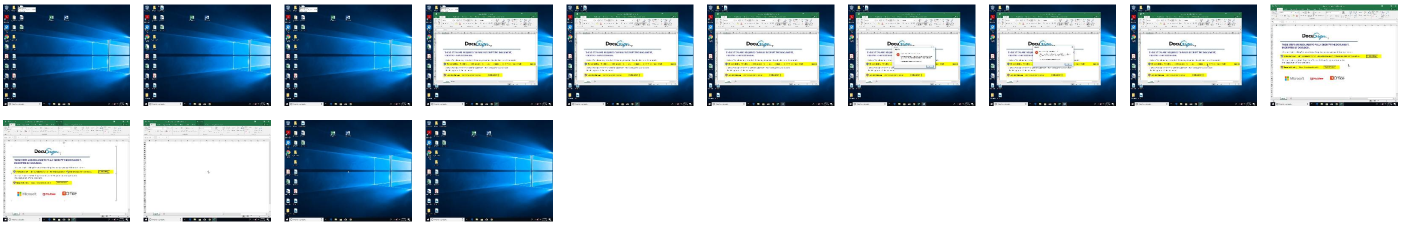
Behavior Graph

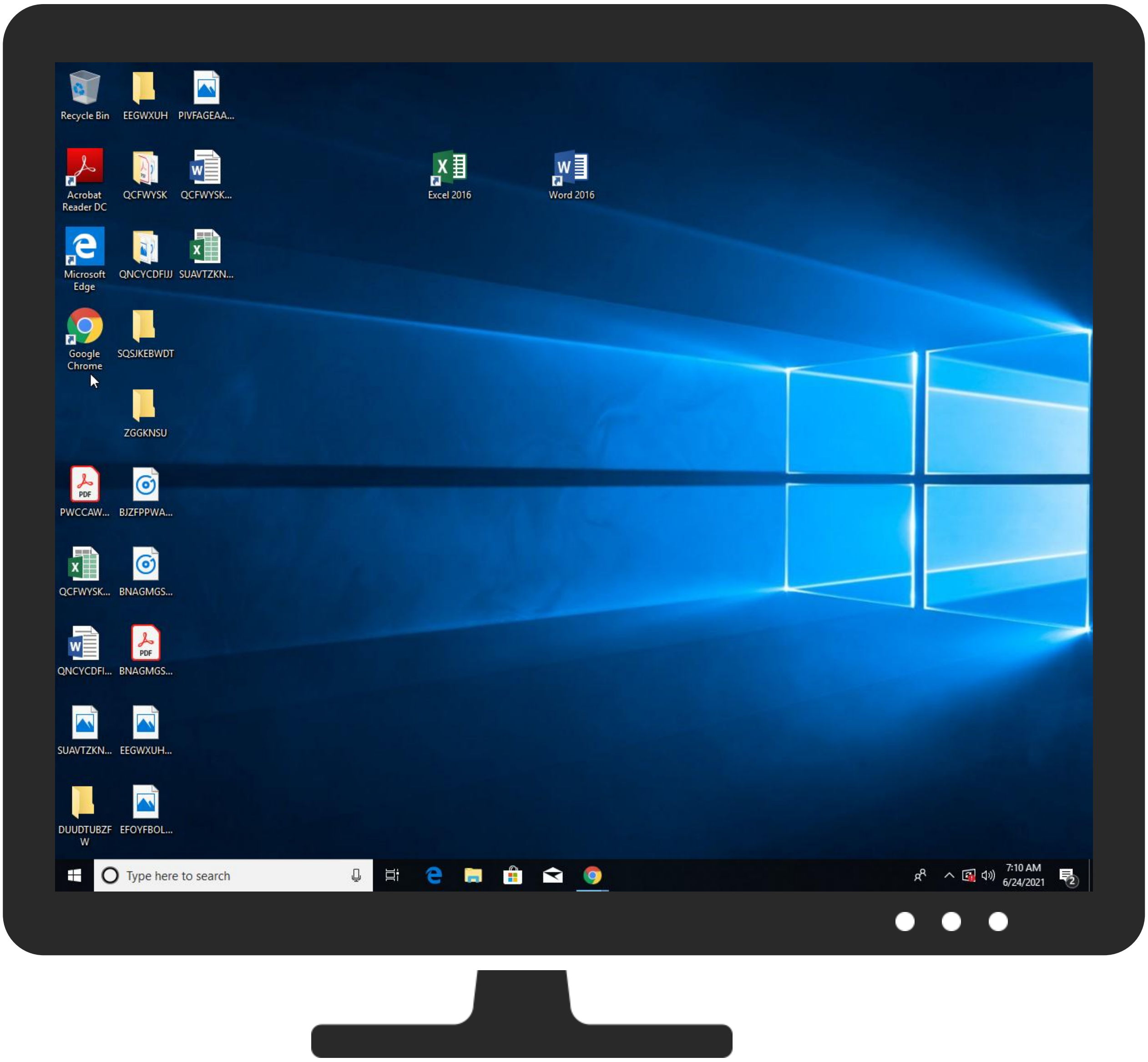


Screenshots

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
carpascapital.com	2%	Virustotal		Browse
gruasphenbogota.com	0%	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	

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://gruasphenbogota.com/C74hwGGxi/ka.html	11%	Virustotal		Browse
http://https://gruasphenbogota.com/C74hwGGxi/ka.html	100%	Avira URL Cloud	malware	
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%	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://carpascapital.com/gBPg8MtsGbv/ka.html%	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	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
carpascapital.com	50.116.92.246	true	false	• 2%, Virustotal, Browse	unknown
gruasphenbogota.com	50.116.92.246	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.116.92.246	carpascapital.com	United States	🇺🇸	46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	439554
Start date:	24.06.2021
Start time:	07:07:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-930205822.xlsb
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
Number of analysed new started processes analysed:	29
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.expl.evad.winXLSB@5/4@2/1
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: .xlsb • 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
50.116.92.246	plan-277786552.xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carpascapital.com	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246
gruasphenbogota.com	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	7UXBXIr31E.exe	Get hash	malicious	Browse	• 192.185.198.10
	TW8o2zNu2Q.exe	Get hash	malicious	Browse	• 50.116.109.135
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 108.167.164.216
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	Order.exe	Get hash	malicious	Browse	• 108.167.183.94
	0rder-bcm_23062021.exe	Get hash	malicious	Browse	• 50.87.249.240
	wdxYcFUCJV.exe	Get hash	malicious	Browse	• 74.220.199.6
	Inv 820984.xlsb	Get hash	malicious	Browse	• 162.144.12.168
	N0vpYgIYpv.exe	Get hash	malicious	Browse	• 162.241.216.218
	droxoUY6SU.exe	Get hash	malicious	Browse	• 192.185.185.25
	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249
	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249
	Fra8994.exe	Get hash	malicious	Browse	• 162.241.60.126

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	mCzW1o1ZtQ.exe	Get hash	malicious	Browse	• 50.116.92.246
	Receipt_ID544663355899706.js	Get hash	malicious	Browse	• 50.116.92.246
	Receipt_ID544663355899706.js	Get hash	malicious	Browse	• 50.116.92.246
	ol3LDsjE6A.exe	Get hash	malicious	Browse	• 50.116.92.246
	ol3LDsjE6A.exe	Get hash	malicious	Browse	• 50.116.92.246
	Z2YNNlDA9o.exe	Get hash	malicious	Browse	• 50.116.92.246
	ZPO1ZXwaGR.exe	Get hash	malicious	Browse	• 50.116.92.246
	T4j76UbWCy.exe	Get hash	malicious	Browse	• 50.116.92.246
	6D03.exe	Get hash	malicious	Browse	• 50.116.92.246
	9i70IpVwXU.exe	Get hash	malicious	Browse	• 50.116.92.246
	update2.zip.exe	Get hash	malicious	Browse	• 50.116.92.246
	Build.exe	Get hash	malicious	Browse	• 50.116.92.246
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	Declaration-Of-Independence-Crossword-Puzzle-Answers-Quizlet.exe	Get hash	malicious	Browse	• 50.116.92.246
	instagrampassword_setup.exe	Get hash	malicious	Browse	• 50.116.92.246
	bmaphis@cardinaltek.com_16465506 AMDocAtt.HTML	Get hash	malicious	Browse	• 50.116.92.246
	twd.exe	Get hash	malicious	Browse	• 50.116.92.246
	0ZQNzv3MyU.exe	Get hash	malicious	Browse	• 50.116.92.246
	USD 12,371.35 SWIFT report.exe	Get hash	malicious	Browse	• 50.116.92.246
	PAYMENT COPY.ppt	Get hash	malicious	Browse	• 50.116.92.246

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\57891FD6-44C4-41E2-9BAC-FD1A025B680A

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):	5.367834958853468
Encrypted:	false
SSDEEP:	1536:bcQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:rEQ9DQW+zvXO1
MD5:	80F44E4B6041D4F709F3096C5D35EA67
SHA1:	0A12CFE1F4BB3B79C8699B4C4591EB1AAFBBF7AE
SHA-256:	80E63F5FEF469A99F9F784E070D8F9F60FDAFA6235C5D6060E6267BF8E26A6AA
SHA-512:	4D34D2645F1F1B61BA7E58A7D28676F7A3595AF03798835F5F09877D0874BF4E44BE0BFF786DC661F5E75540A83386462F7FFCAFABBFBDCF017FA1CD01C36D3
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="2021-06-24T05:08:10">.. Build: 16.0.14222.30527-->.. <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\FCD3AD83.png

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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FCD3AD83.png

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.*.$H.B.P.)l.6Q..'.l..7..k..J.o..._....6..{C...r.\|2W.[a...m.Bl.?...5......D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._.,..I.\|a.7+>.........A#......3v..37......w(..j...C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..\|..d../.......vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.......#!...T...C.#.>.E,[.,......E....h~B.Y./....(2.......(...`....~w#.%..R..{........N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q.."...W2.......Q...G...z....Ea......

C:\Users\user\AppData\Local\Temp\75810000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	113222
Entropy (8bit):	7.875738732899415
Encrypted:	false
SSDEEP:	1536:PKYUOtOpEknvGrnxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncVd:PKY45br0o45GUgHhX8jC9ySVd
MD5:	04EC9A165F91EEEC2E1A16D7D458083E
SHA1:	DE28E006BB4E61BEE221F2AED03D3126AB2AECE6
SHA-256:	5BC4685E6B2D3D3AE48640631C40E4DF03CD9D0E8244D55CD71C365AD07C3A3D
SHA-512:	6ECE536BD31A66300CFACEA3B7A90D452DD2950DD3838C89E123B5B3080490B9BBB423C90B341411425E60C1324278325454AFBCAF189F3E37C53A971A017DE
Malicious:	false
Reputation:	low
Preview:	...N.1....x...h.EUU..h. .>..>.X.M>....3....U......./....#&2.........U/~..h...2x.6x...l\-.>....a..^.9.R....u!..eH.2......By9.}.*..>..x...;.....z..;..W....W.za\.vyP......h...s..^..jG...u..&.9..#...fz.0.nx1....B.?.1..X....>.uw.P:jq..v4 ..J...E.....$U%...xG...k.ri....oSG1!.j.lWfR.'8*..b|.......L.e>z(....W..@.[.....3.J. ....?N_...X.....".%...W....l.)..W....'r....X.8..@..W..........PK..........!.j.9............[Content_Types].xml ...(...MO.0...H......

C:\Users\user\Desktop\~$plan-930205822.xlsb

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.836343677163856

General

TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	plan-930205822.xlsb
File size:	90078
MD5:	a9632052eafc78ee7e2225a59aefa468
SHA1:	2bade21221f175cda46c2d819746674579f28f2d
SHA256:	ae39ed7fd03aae627c65cdb4d7fb0a938fc4f328e2611da087589cc57ca7c3dd
SHA512:	456e69cd6a23c6a0011a50d3e8ba71314b3b33c59f9c1d71430fc821bb48239257c8622f48f18c7ffa8a0475c269086035efa7c7a1024e6c687c33f382779845
SSDEEP:	1536:4lHoxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncjv0/Ci:ADbr0o45GUgHhX8jC9ySa
File Content Preview:	PK..........!..#..............[Content_Types].xml ...(..

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "plan-930205822.xlsb"

Indicators

Has Summary Info:	
Application Name:	
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

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 24, 2021 07:08:13.108743906 CEST	192.168.2.3	8.8.8.8	0xf071	Standard query (0)	carpascapital.com	A (IP address)	IN (0x0001)
Jun 24, 2021 07:08:14.431987047 CEST	192.168.2.3	8.8.8.8	0xca6c	Standard query (0)	gruasphenbogota.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2021 07:08:13.166194916 CEST	8.8.8.8	192.168.2.3	0xf071	No error (0)	carpascapital.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 24, 2021 07:08:14.487782955 CEST	8.8.8.8	192.168.2.3	0xca6c	No error (0)	gruasphenbogota.com		50.116.92.246	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 24, 2021 07:08:13.510010958 CEST	50.116.92.246	443	192.168.2.3	49715	CN=*.carpascapital.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.	Fri May 21 05:30:14 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 05:30:14 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		
Jun 24, 2021 07:08:14.905570984 CEST	50.116.92.246	443	192.168.2.3	49718	CN=gruasphenbogota.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.	Mon May 10 05:47:53 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 05:47:53 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: 5716 Parent PID: 792

General

Start time:	07:08:09
Start date:	24/06/2021
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:	0x390000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 4220 Parent PID: 5716

General

Start time:	07:08:15
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi1.dll
Imagebase:	0xc0000
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: 1956 Parent PID: 5716

General

Start time:	07:08:16
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi2.dll
Imagebase:	0x7ff77db90000
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