ID: 439114
Sample Name: plan-277786552.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 18:05:43
Date: 23/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

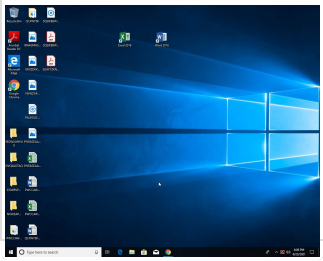
Windows Analysis Report plan-277786552.xlsb

Overview

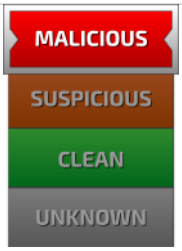
General Information

Sample Name:	plan-277786552.xlsb
Analysis ID:	439114
MD5:	1ab505496be60c..
SHA1:	2a2602511286c9..
SHA256:	af9ed7ee18c7898.
Infos:	

Most interesting Screenshot:



Detection



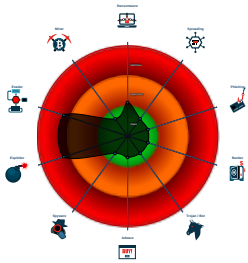
Hidden Macro 4.0

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: 1056 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 3840 cmdline: regsvr32 ..\gihi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5988 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)

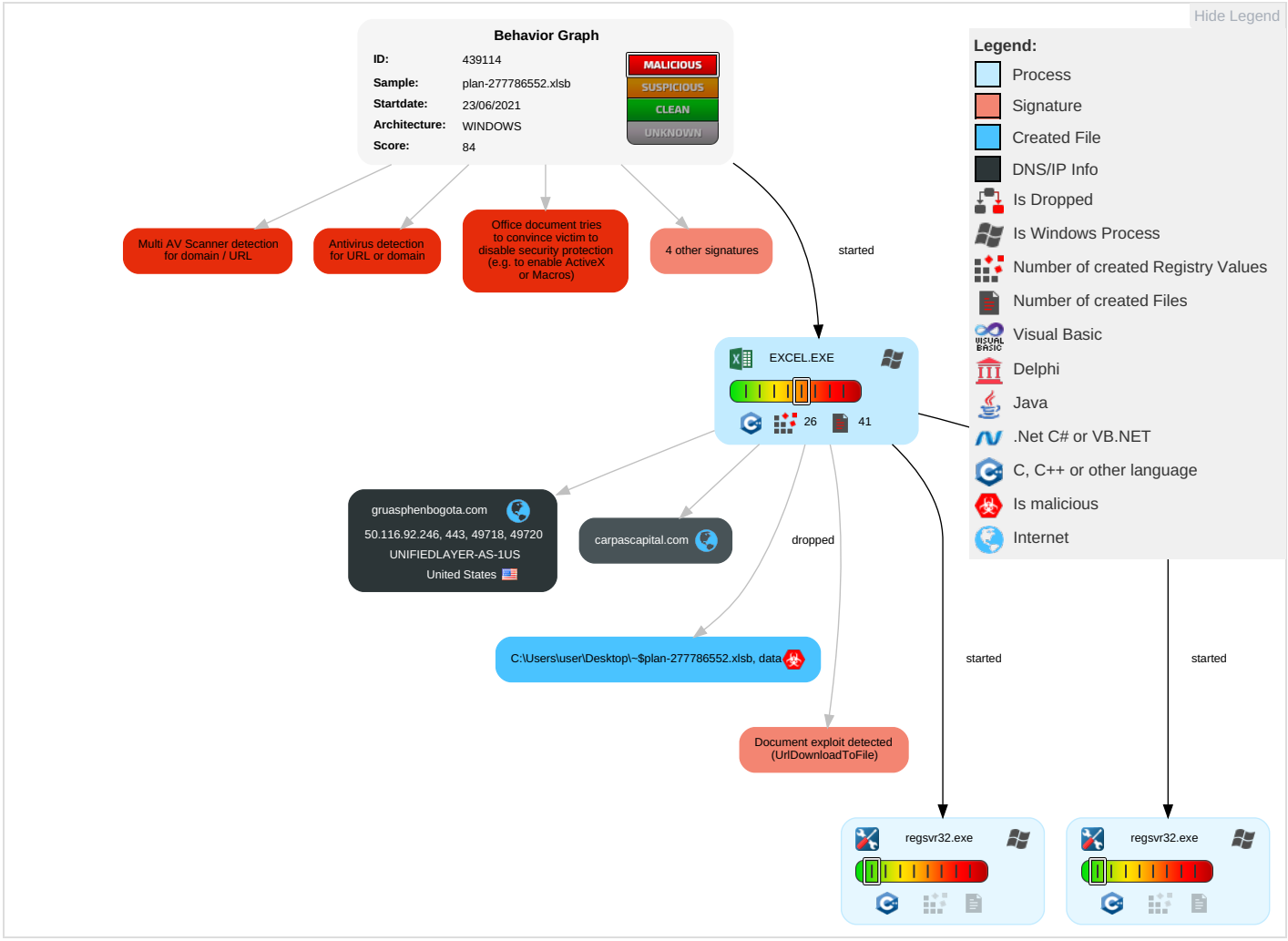
Found Excel 4.0 Macro with suspicious formulas

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	Regsvr32 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
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 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)	Process Injection 1	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	Scripting 2	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	

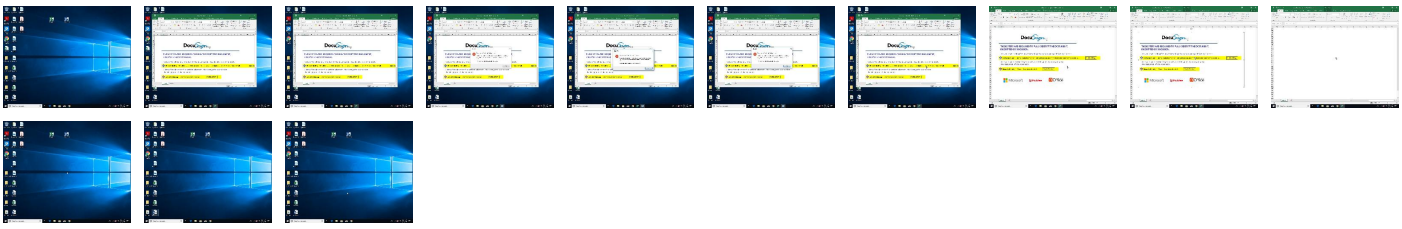
Behavior Graph



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	7%	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:	439114
Start date:	23.06.2021
Start time:	18:05:43
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-277786552.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

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	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
	20210621_064143.html	Get hash	malicious	Browse	• 50.116.92.246
	Wire Info.docx	Get hash	malicious	Browse	• 50.116.92.246
	Nueva orden de env#U00edo .exe	Get hash	malicious	Browse	• 50.116.92.246
	Global _Transport NZ..xlsx	Get hash	malicious	Browse	• 50.116.92.246
	ghXWqV6o1J.docx	Get hash	malicious	Browse	• 50.116.92.246
	idea-22543577.xlsm	Get hash	malicious	Browse	• 50.116.92.246
	OzygoxrbzzvtmyjupcpndcovpjxtqpiywjSigned.exe	Get hash	malicious	Browse	• 50.116.92.246
	2t71031BUz.exe	Get hash	malicious	Browse	• 50.116.92.246
	DmtxjmmsiwawliehhrzxcpwdxtexpegwgoSigned.exe	Get hash	malicious	Browse	• 50.116.92.246
	tender-1235416393.xlsm	Get hash	malicious	Browse	• 50.116.92.246
	Payment Ref 24,845.docx	Get hash	malicious	Browse	• 50.116.92.246
	3yBar59k6g.exe	Get hash	malicious	Browse	• 50.116.92.246
	rVkZUqVZ40.exe	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\5BE7D80B-BB37-4BDA-B35D-5B3F7A73C206	
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):	5.367833155181977
Encrypted:	false
SSDEEP:	1536:ecQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:KEQ9DQW+zvXO1
MD5:	C4D761BF1A56A083F277A1150EF05D9C
SHA1:	AD44052E997E92F86B56D894CFAE334EF0B681DC
SHA-256:	8612616C102A5B84C2DDD60E5B3BC3F214FE74CCE6984E6372B6315F37D5B540
SHA-512:	F4524498E75321F646BA8E3A01CF27373FD2C0BB0629BCA1E9EC7DC1D12D8B1DB3E9C5980F31F207D6209C5C56A2466D82422E2C6CDB6B98EDE236B70F481AB
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="2021-06-23T16:06:37">.. 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\75F7EE28.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\75F7EE28.png	
Size (bytes):	75711
Entropy (8bit):	7.915372969602997
Encrypted:	false
SSDEEP:	1536:gxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncT:7br0o45GUgHhX8jC9yST
MD5:	8296338A43942E3107802E3062AC1270
SHA1:	46E67A586ED8A961AF7FD03140547C1CB2BAC227
SHA-256:	BE5F61F2AE8E4C9F9ADBCE5EC33D4C01A331734FFC5818AA8E45CF60456C5ABD
SHA-512:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171AD
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.*.$H.B.P.)l.6Q..'.l..7..k..J.o..._....6..{C...r.\|2W.[a...m.BI.?...5.....D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._.,..I.\|a.7+>.....A#.....3v..37.....w(..j.. .C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..\|..d../.....vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.....#!...T...C.#.>.E,[,.....E....h~B.Y./....(2.....(..`....~w#.% ..R..{.....N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q.."...W2.....Q...G...z....Ea.....

C:\Users\user\AppData\Local\Temp\0E810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	113222
Entropy (8bit):	7.875705327761934
Encrypted:	false
SSDEEP:	1536:PKYUOtOpEknvGrnxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncVv:PKY45br0o45GUgHhX8jC9ySVv
MD5:	8C848255DE789AD5D1608009EEE15D33
SHA1:	08A3F58BE98F761E7D5DFC32B696883C2A73BCE8
SHA-256:	A4A401D633D6F597AB78A8BA222FAAEC0AC20C59C650FBC4B79ED9E4ACE2E213
SHA-512:	E716087902546951548 31E942E4DCD97F54BB885971E9DB7F833635C2686830858611BE3D1B8922750411512D0FF7D1A34854329448D5695DCEC4067614807DF
Malicious:	false
Reputation:	low
Preview:	...N.1....x...h.EUU..h. .>..>.X.M>....3....U...../....#&2.....U/~..h...2x.6x...I\->....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.IWfR.'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-277786552.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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
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):	7.83635013932937

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-277786552.xlsb
File size:	90078
MD5:	1ab505496be60c9ec06e78052d5cf557
SHA1:	2a2602511286c90591824cf91b1027f20e537212
SHA256:	af9ed7ee18c789857f7356314109cf0635f6905afc9a6ad74f8742c78d46b446
SHA512:	6f8358e59793837918765d183e28a4d4cc5afd4cc9c216bb1e91b6288f523b478505f5e8532d924c379742956ebc185f8e22464cd5efdbf685773e9c9076fc79
SSDEEP:	1536:KlHoxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncjv0/Ci:KDbr0o45GUgHhX8jC9ySa
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-277786552.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 23, 2021 18:06:39.846254110 CEST	192.168.2.3	8.8.8.8	0x7c0a	Standard query (0)	carpascapital.com	A (IP address)	IN (0x0001)
Jun 23, 2021 18:06:40.810590029 CEST	192.168.2.3	8.8.8.8	0x6e45	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 23, 2021 18:06:39.893533945 CEST	8.8.8.8	192.168.2.3	0x7c0a	No error (0)	carpascapital.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 23, 2021 18:06:40.866476059 CEST	8.8.8.8	192.168.2.3	0x6e45	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 23, 2021 18:06:40.216695070 CEST	50.116.92.246	443	192.168.2.3	49718	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 23, 2021 18:06:41.195301056 CEST	50.116.92.246	443	192.168.2.3	49720	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: 1056 Parent PID: 792

General

Start time:	18:06:35
Start date:	23/06/2021
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:	0x1330000
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: 3840 Parent PID: 1056

General

Start time:	18:06:41
Start date:	23/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi1.dll
Imagebase:	0x1e0000
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: 5988 Parent PID: 1056

General

Start time:	18:06:42
Start date:	23/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi2.dll
Imagebase:	0x1e0000
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