ID: 442411
Sample Name: plan-870783614.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:48:45
Date: 30/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

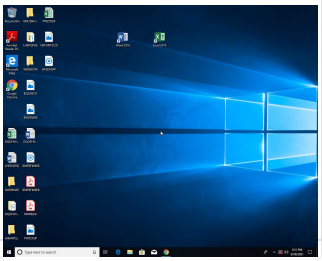
Windows Analysis Report plan-870783614.xlsb

Overview

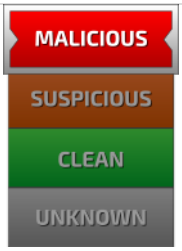
General Information

Sample Name:	plan-870783614.xlsb
Analysis ID:	442411
MD5:	b95aefeb399b695.
SHA1:	3793372eea233d..
SHA256:	ac59fec5c5a1571..
Infos:	

Most interesting Screenshot:



Detection



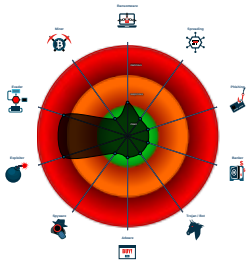
Hidden Macro 4.0

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- 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…
- Registers a DLL
- Tries to load missing DLLs

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6884 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5920 cmdline: regsvr32 ..\gihi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5960 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

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)

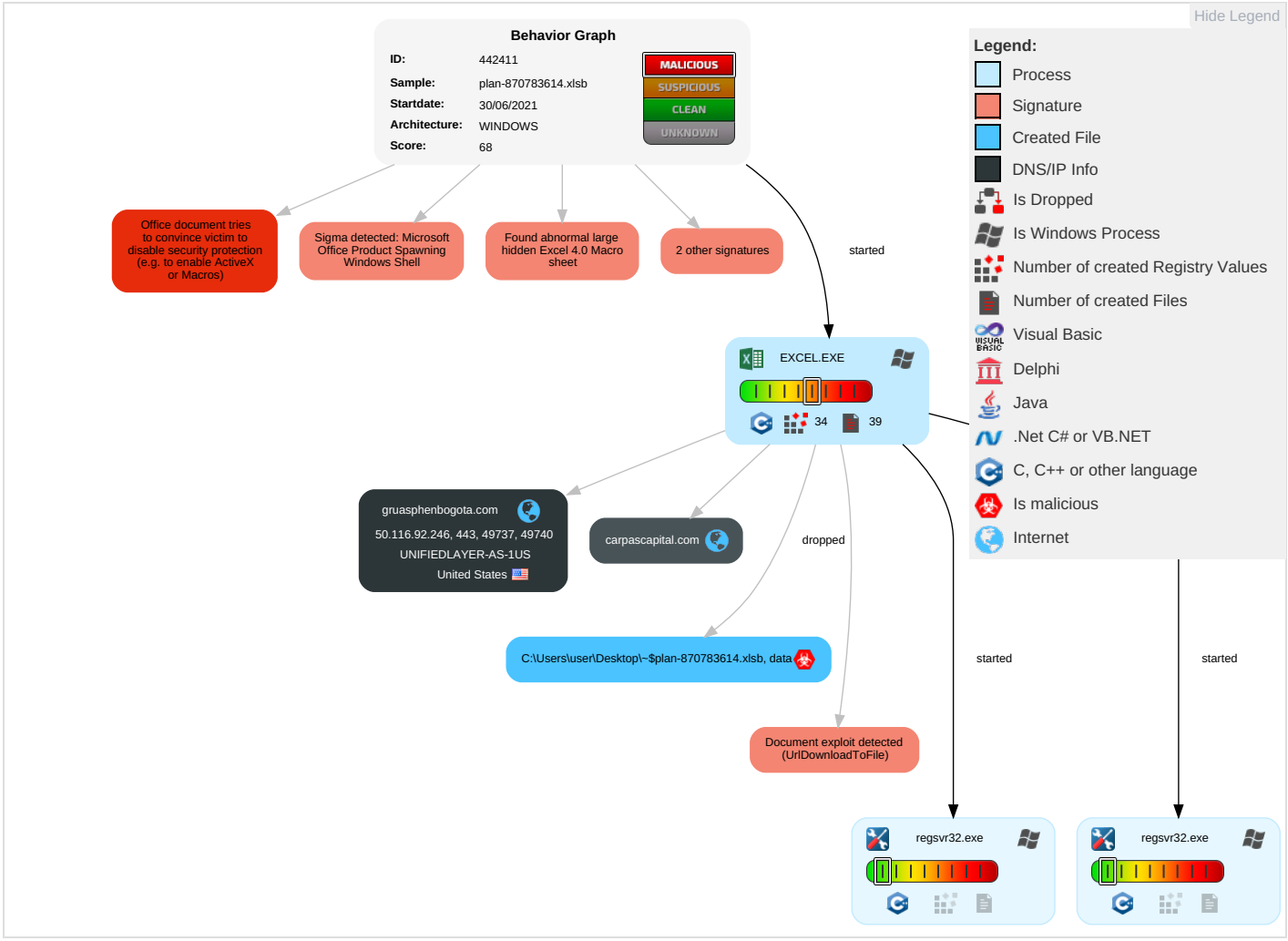
Found Excel 4.0 Macro with suspicious formulas

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	

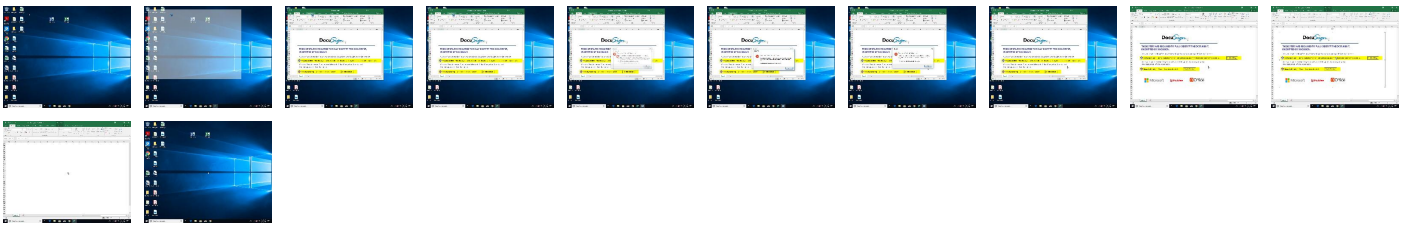
Behavior Graph



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	5%	Virustotal		Browse
gruasphenbogota.com	5%	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	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://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	
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	

Source	Detection	Scanner	Label	Link
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	• 5%, Virustotal, Browse	unknown
gruasphenbogota.com	50.116.92.246	true	false	• 5%, 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:	442411
Start date:	30.06.2021
Start time:	15:48:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-870783614.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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal68.expl.evad.winXLSB@5/5@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-1053707320.xlsb	Get hash	malicious	Browse	
	plan-1053707320.xlsb	Get hash	malicious	Browse	
	plan-930205822.xlsb	Get hash	malicious	Browse	
	plan-277786552.xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carpascapital.com	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246
gruasphenbogota.com	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	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	SecuriteInfo.com.Trojan.PackedNET.899.26593.exe	Get hash	malicious	Browse	• 192.185.171.219
	S9zNklNfAS.exe	Get hash	malicious	Browse	• 162.241.253.69
	po_order_item_29062021.exe	Get hash	malicious	Browse	• 162.241.30.109
	Viaseating Copy.html	Get hash	malicious	Browse	• 69.49.228.180
	diagram-1878769052.xls	Get hash	malicious	Browse	• 192.185.195.245
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	newbad.rtf_Client.vbs	Get hash	malicious	Browse	• 50.116.92.246
	spot.dll	Get hash	malicious	Browse	• 50.116.92.246
	spot.dll	Get hash	malicious	Browse	• 50.116.92.246
	3.dll	Get hash	malicious	Browse	• 50.116.92.246
	3.dll	Get hash	malicious	Browse	• 50.116.92.246
	StsDQGUVmT.exe	Get hash	malicious	Browse	• 50.116.92.246
	L0DdbYIYEx.exe	Get hash	malicious	Browse	• 50.116.92.246
	GamDzCDMI0.exe	Get hash	malicious	Browse	• 50.116.92.246
	O8O8CUUvAF.exe	Get hash	malicious	Browse	• 50.116.92.246
	1.htm	Get hash	malicious	Browse	• 50.116.92.246
	plan-515372324.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	djBbDPfGV3.exe	Get hash	malicious	Browse	• 50.116.92.246
	CMXz729xzg.exe	Get hash	malicious	Browse	• 50.116.92.246
	#Ud83d#Udcde_#U25b6Play_to_Listen.htm	Get hash	malicious	Browse	• 50.116.92.246
	jssloader.exe	Get hash	malicious	Browse	• 50.116.92.246
	gYbyE02c71.exe	Get hash	malicious	Browse	• 50.116.92.246
	Copy of Check.html	Get hash	malicious	Browse	• 50.116.92.246
	diagram-1878769052.xls	Get hash	malicious	Browse	• 50.116.92.246
	statistic-1496367785.xls	Get hash	malicious	Browse	• 50.116.92.246
	Bank_ details.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\ABEE3621-D8E4-4A15-84D9-852382602615	
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):	135209
Entropy (8bit):	5.363078436709489
Encrypted:	false
SSDEEP:	1536:/cQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:DEQ9DQW+zwXO1
MD5:	9364106DD61DE5E5340275EEC4CEA8A5
SHA1:	E3618AB25C8E8873E5F94CA5990E91A70D502B78
SHA-256:	8D0ED5594AC230E90E88834D30445F00E8A2BCC0908AF292B68FAE9EABC28447
SHA-512:	EE5CC4ADD95FA02613189CE5AC5B3EC79A715D2B85700149EA9C34A680588BB5E6404E1EFF58BB2743624C93ECDC62FDC83E81392E6E4F53D059CAFFBE8AB403
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="2021-06-30T13:49:35">.. Build: 16.0.14228.30525-->.. <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\DD87128.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:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171AD
Malicious:	false
Reputation:	moderate, very likely benign file
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\88A40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	113223
Entropy (8bit):	7.875667152615629
Encrypted:	false
SSDEEP:	1536:PKYUOtOpEknvGrnxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncV/:PKY45br0o45GUgHhX8jC9ySV/
MD5:	1508E45147536467800864C68517467A
SHA1:	EC9A8496B7DF330E59772813EBE9E1F83D2D3F07
SHA-256:	DB72D6AD57573774A8395F44912F81780002E410F79F373E2AC3581E9DE66809
SHA-512:	949B47BA8019C7A86932BAC6E84AE93066AEB08B72C30B1FB7761AB34877D48C5012142804AE90D1C4BAD79D544C2B9D5FDD5B0D6527323B822220E429818616
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....I.)..W....'r....X.8..@..W.....PK..... ....!.j.9.....[Content_Types].xml ...(..... ....MO.0...H.....

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$plan-870783614.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:RFXl6dtt:RJ1

C:\Users\user\Desktop\~$plan-870783614.xlsb	
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):	7.836354041987806
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-870783614.xlsb
File size:	90078
MD5:	b95aefeb399b6956438c6ad0f364ac2b
SHA1:	3793372eea233de7e8efaa91fee58e1aa81eafc1
SHA256:	ac59fec5c5a15711b732a7a9194e6a15bb23b592beebaa e9a2448457c36511d6
SHA512:	088e1911ea096a46db38dfaab0ead4ce4ed7c9e53cfbcb8 1344a58b33616faba0157d49b142616b057a3edd3dda54 8fddeae836036c127e45369409c9893dbe9
SSDEEP:	1536:ilHoxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl 5ncjv0/Ci:iDbr0o45GUgHhX8jC9ySa
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-870783614.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
Jun 30, 2021 15:49:38.159046888 CEST	192.168.2.4	8.8.8.8	0xbdb8	Standard query (0)	carpascapital.com	A (IP address)	IN (0x0001)
Jun 30, 2021 15:49:40.807324886 CEST	192.168.2.4	8.8.8.8	0x75b	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 30, 2021 15:49:38.217343092 CEST	8.8.8.8	192.168.2.4	0xbdb8	No error (0)	carpascapital.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 30, 2021 15:49:40.864131927 CEST	8.8.8.8	192.168.2.4	0x75b	No error (0)	gruasphenbogota.com		50.116.92.246	A (IP address)	IN (0x0001)

HTTPS Packets

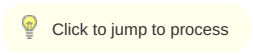
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 30, 2021 15:49:38.706794977 CEST	50.116.92.246	443	192.168.2.4	49737	CN=*.carpascapital.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research 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 30, 2021 15:49:41.362982035 CEST	50.116.92.246	443	192.168.2.4	49740	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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



System Behavior

Analysis Process: EXCEL.EXE PID: 6884 Parent PID: 800

General

Start time:	15:49:33
Start date:	30/06/2021
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:	0xb60000
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: 5920 Parent PID: 6884

General

Start time:	15:49:44
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi1.dll
Imagebase:	0xb70000
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: 5960 Parent PID: 6884

General

Start time:	15:49:45
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi2.dll
Imagebase:	0xb70000
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