

JOeSandbox Cloud BASIC



ID: 438318

Sample Name: plan-
1637276620.xlsm

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 13:33:24

Date: 22/06/2021

Version: 32.0.0 Black Diamond

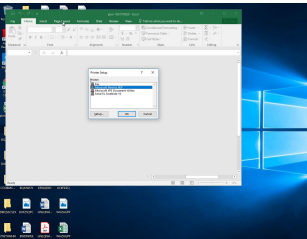
Table of Contents

Table of Contents	2
Windows Analysis Report plan-1637276620.xlsm	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Signature Overview	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	4
Thumbnails	4
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	7
Contacted Domains	7
URLs from Memory and Binaries	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	9
General	9
File Icon	10
Network Behavior	10
Network Port Distribution	10
UDP Packets	10
Code Manipulations	10
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: EXCEL.EXE PID: 7120 Parent PID: 800	10
General	10
File Activities	11
File Written	11
Registry Activities	11
Analysis Process: splwow64.exe PID: 4292 Parent PID: 7120	11
General	11
File Activities	11
Disassembly	11

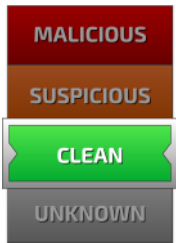
Windows Analysis Report plan-1637276620.xlsm

Overview

General Information

Sample Name:	plan-1637276620.xlsm
Analysis ID:	438318
MD5:	4d44784f088b8dd.
SHA1:	7d01c190b2e73c..
SHA256:	c63e0b01a696a0..
Infos:	
Most interesting Screenshot:	
	

Detection

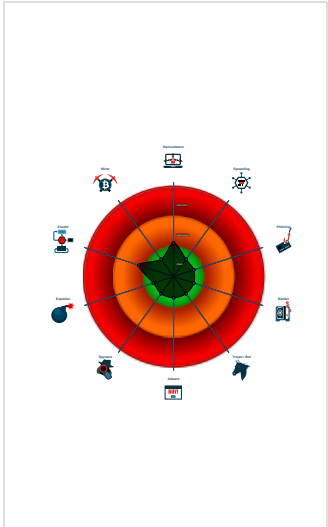


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

Excel documents contains an embe...

Classification



Process Tree

- System is w10x64
-  EXCEL.EXE (PID: 7120 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
 -  splwow64.exe (PID: 4292 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

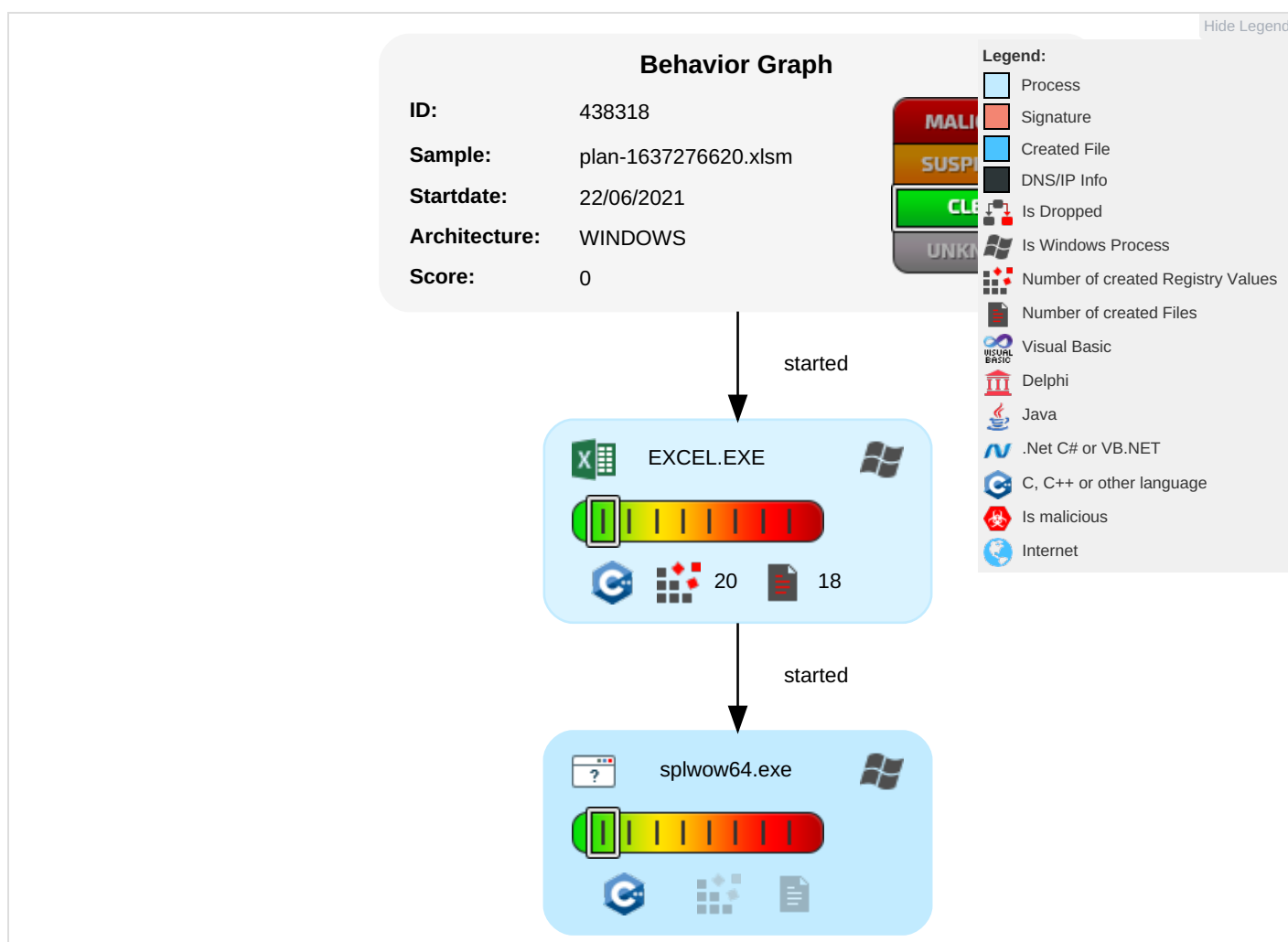
 Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

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 Services
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remote Tracking Without Authn
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Without Authn
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

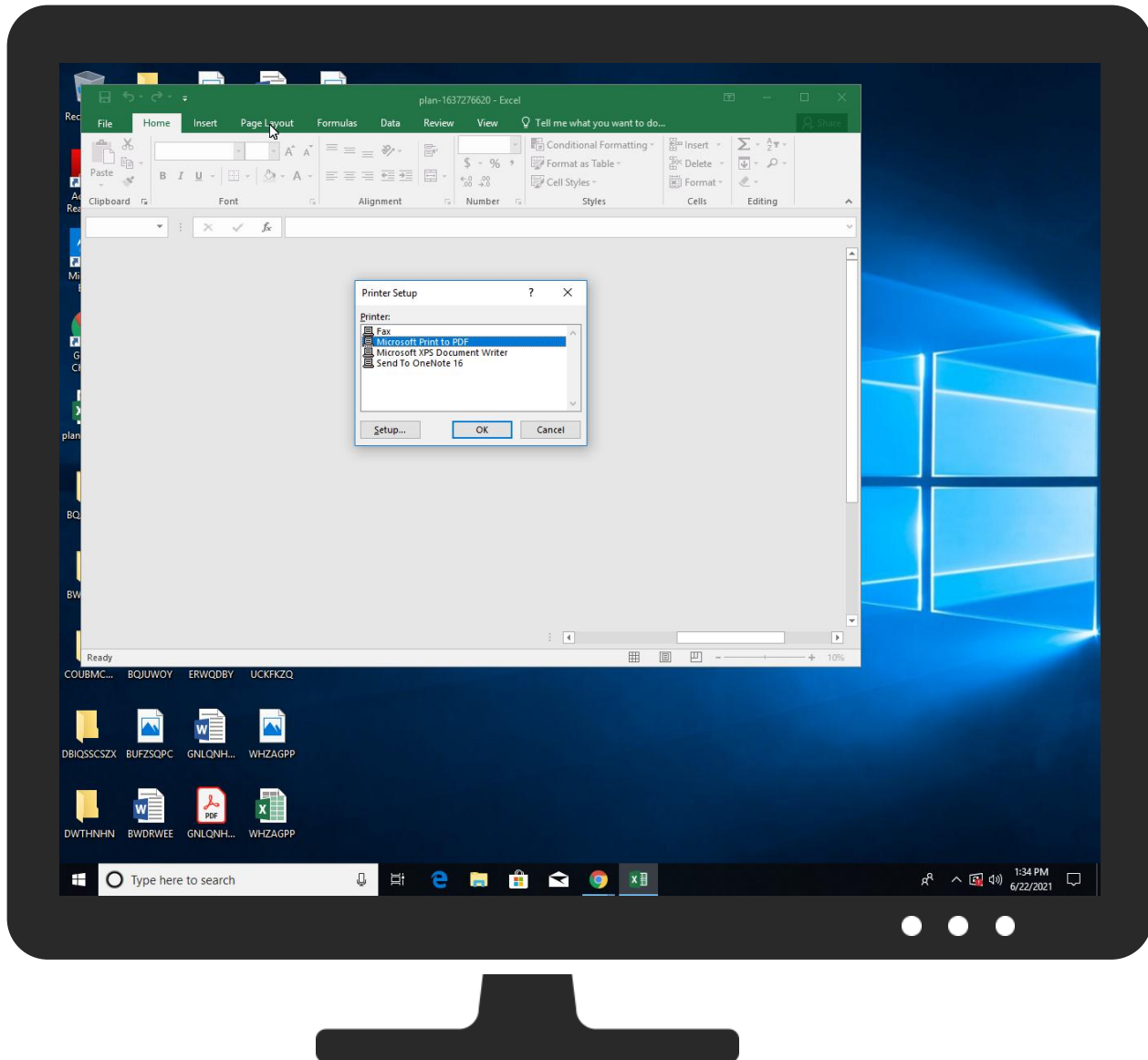
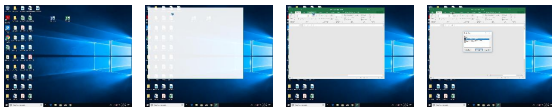
Behavior Graph



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
plan-1637276620.xlsm	2%	Virustotal		Browse

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

Source	Detection	Scanner	Label	Link
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://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgmsproxyapi.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://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://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://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://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://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	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	438318
Start date:	22.06.2021
Start time:	13:33:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 56s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-1637276620.xlsm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	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:	CLEAN
Classification:	clean0.winXLSM@3/3@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsm
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:34:24	API Interceptor	20x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2CAF7AE8-289A-4F25-868B-6D2546F9329C	
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):	5.367807218977918
Encrypted:	false
SSDEEP:	1536:vcQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWxboOidX5E6LWME9:vEQ9DQW+zvXO1
MD5:	0D48EA4DD74C64C5A1C57AD28FFBCABF
SHA1:	B1734754C9B1D84A250FA2B1D238F49707A55A17
SHA-256:	D09E1FCDBF132DBE299FBE0909F3B446B008B32EEECAC756898747BF845C31050
SHA-512:	A7A4531B0237FD5211DAA23F5B4747A8A8B36B93BD3F8E4C76BF6BC7AF26FC16FC1AA5EE801A298DDCAD2DC60EDD62C950A200EBE48052FB87A516CF7A004F6D
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="2021-06-22T11:34:20">..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.aspx</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="CIViewClientHelpId">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientHome">..<o:url>https://[MAX.BaseHost]/client/results</o:url>..</o:service>..<o:service o:name="CIViewClientTemplate">..<o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>..</o:service>..<o:

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\Content.MSO\DF8B976F.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:gxJQVqyZEbrMj34410mHyL9c988gHhX8jCNnKf5ncT: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.lf.,ffX1K.[...Z...V.LO5L..J+...z.]]u...>==.....Q.....(.....p.t.....8.....g@G.....3.....(.....p.t.....8.....g@G.....3.....Q.....(.....p.t.....j.7ZP...0S...z5T.....).WU= .*.\$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....(.....l.j.a.7+>.....A#.....3v...37.....w(.j..C.R..H3.f.Q....0...h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..j..d../.....vC..&..=9...n....^6-.tRj...O..fj.e.N....o..~.^.....#1...T..C.#>.E.[.....E....h-B.Y./....(2.....(.....~w#.%..R..{.....N.Z....k]8>..dW..^s...U...9...W.e...j...W...i.{u.>s.,L,>1..}....f..b..Z.nai\$Q.."...W2.....Q...G...z....Ea.....

C:\Users\user\Desktop-\$plan-1637276620.xlsm	
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:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..pratesh.....p.r.a.t.e.s.h.....

Static File Info

General	
File type:	Microsoft Excel 2007+

General

Entropy (8bit):	7.835274324451968
TrID:	- Excel Microsoft Office Open XML Format document (40004/1) 83.33% - ZIP compressed archive (8000/1) 16.67%
File name:	plan-1637276620.xlsm
File size:	93191
MD5:	4d44784f088b8dd2ac0a6cbf2b809eab
SHA1:	7d01c190b2e73c860a9aed904729c6466230bd26
SHA256:	c63e0b01a696a077a5709b8aa4d4d600344fc1ddba624cbd67c6f37f271d97ac
SHA512:	09c221b8d32ff3a0cb092789103d54ef64b1dffa92a1cdb7047436c6d9e578ee505457d327a55f1dac5f6b2bcd934c80b025b92b50da12ecdc3187e86efa6b69
SSDEEP:	1536:aY2xJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfI5ncW3SLBT0Ca:aYRbr0o45GUgHhX8jC9ySWCLBI
File Content Preview:	PK.....!!=J.....[Content_Types].xml ...({.....

File Icon



Icon Hash:	74ecd0e2f696908c
------------	------------------

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7120 Parent PID: 800

General

Start time:	13:34:18
-------------	----------

Start date:	22/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xb90000
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 Written

Registry Activities

Show Windows behavior

Analysis Process: splwow64.exe PID: 4292 Parent PID: 7120

General

Start time:	13:34:24
Start date:	22/06/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff643fd0000
File size:	130560 bytes
MD5 hash:	8D59B31FF375059E3C32B17BF31A76D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Disassembly