ID: 442112
Sample Name: plan-515372324.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 00:07:35
Date: 30/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

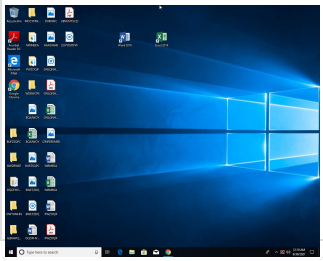
Windows Analysis Report plan-515372324.xlsb

Overview

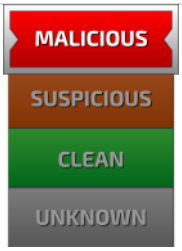
General Information

Sample Name:	plan-515372324.xlsb
Analysis ID:	442112
MD5:	08e52afbefa423f…
SHA1:	2d688dfee28f755..
SHA256:	aaa32ff3e41c61f…
Infos:	

Most interesting Screenshot:



Detection



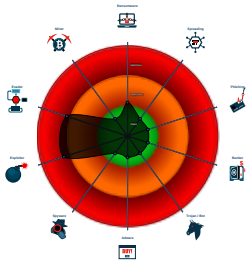
Hidden Macro 4.0

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found abnormal large hidden Excel …
- Sigma detected: Microsoft Office Pr…
- Found a high number of Window / Us…
- JA3 SSL client fingerprint seen in co…
- Monitors certain registry keys / valu…
- Potential document exploit detected…
- Potential document exploit detected…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6272 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - splwow64.exe (PID: 6156 cmdline: C:\Windows\splwow64.exe 12288 MD5: 8D59B31FF375059E3C32B17BF31A76D5)
  - regsvr32.exe (PID: 6464 cmdline: regsvr32 ..\palpy1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 6672 cmdline: regsvr32 ..\palpy2.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:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

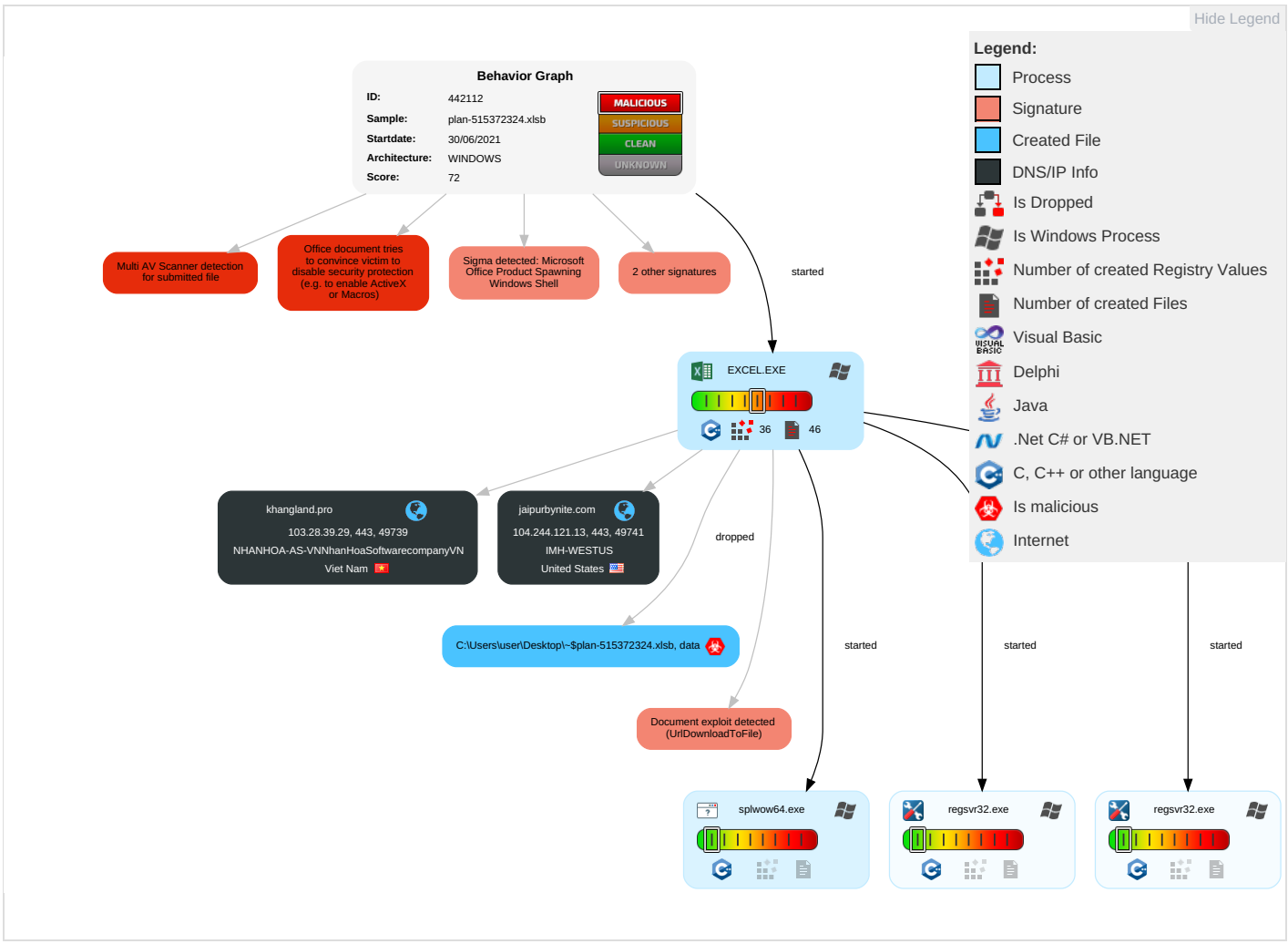
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found 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
Valid Accounts	Scripting 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communicatior
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatior
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	System Information Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

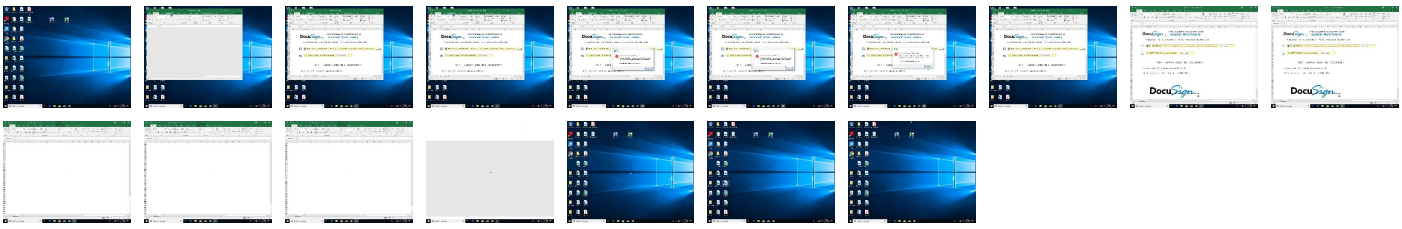
Behavior Graph



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

Source	Detection	Scanner	Label	Link
plan-515372324.xlsb	15%	Virustotal		Browse
plan-515372324.xlsb	22%	ReversingLabs	Document-Office.Backdoor.Quakbot	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
khangland.pro	0%	Virustotal		Browse
jaipurbynite.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	
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://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://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%	Virustotal		Browse
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://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
khangland.pro	103.28.39.29	true	false	• 0%, Virustotal, Browse	unknown
jaipurbynite.com	104.244.121.13	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.244.121.13	jaipurbynite.com	United States		22611	IMH-WESTUS	false
103.28.39.29	khangland.pro	Viet Nam		131353	NHANHOA-AS-VNNhanHoaSoftwarecompanyVN	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	442112
Start date:	30.06.2021
Start time:	00:07:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-515372324.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.expl.evad.winXLSB@7/10@2/2
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

Time	Type	Description
00:08:25	API Interceptor	1155x Sleep call for process: splwow64.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.28.39.29	plan-536150726.xlsb	Get hash	malicious	Browse	
	http://https://otochothue.com/ahead/89963/89963.zip	Get hash	malicious	Browse	
	http://https://otochothue.com/ahead/20376640/20376640.zip	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
khangland.pro	plan-536150726.xlsb	Get hash	malicious	Browse	• 103.28.39.29

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IMH-WESTUS	dqVPlpmWYt.exe	Get hash	malicious	Browse	• 74.124.211.132
	chems.exe	Get hash	malicious	Browse	• 192.249.117.18
	Mohamed Abrar H CV.xlsx	Get hash	malicious	Browse	• 205.134.252.239
	INVOICE125POR.xlsx	Get hash	malicious	Browse	• 205.134.252.239
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 104.247.72.46
	PACKING LIST CORP INVOICE 2738829 DATED 26 FOR SHIPMENT AS STATED ON 26 APRIL05l992lcNll.exe	Get hash	malicious	Browse	• 192.145.239.54
	PACKING LIST CORP INVOICE 2738829 DATED 26 FOR SHIPMENT AS STATED ON 26 APRIL05l992lc.exe	Get hash	malicious	Browse	• 192.145.239.54
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 104.247.72.46
	PACKING LIST CORP INVOICE 2738829 DATED 26 FOR SHIPMENT AS STATED ON 26 APRIL05l.exe	Get hash	malicious	Browse	• 192.145.239.54
	Telex.exe	Get hash	malicious	Browse	• 192.145.239.54
	PO 367628usa.exe	Get hash	malicious	Browse	• 209.182.202.96
	eLECTRONIC Flight Ticket Invoice confirmationETKT XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	eLECTRONIC Flight Ticket Confirmation VIS XXXXX3939 INVOICE 000Z1298932 TKT Payment.exe	Get hash	malicious	Browse	• 192.145.239.54
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	scan of bill 0905.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	PO9448882.exe	Get hash	malicious	Browse	• 209.182.202.96
	check 6746422.xlsm	Get hash	malicious	Browse	• 192.249.126.181
	TKT eLECTRONIC Flight Ticket Confirmation VIS XXXX X83939 INVOICE 000Z1298932 TKT.exe	Get hash	malicious	Browse	• 192.145.239.54
	proforma invoice.exe	Get hash	malicious	Browse	• 192.249.124.39
NHANHOA-AS-VNNhanHoaSoftwarecompanyVN	dLIF0bPWxx.exe	Get hash	malicious	Browse	• 103.28.36.10
	eNjlpT5RzD.exe	Get hash	malicious	Browse	• 103.28.36.10
	Plq7ADczmp.exe	Get hash	malicious	Browse	• 103.28.36.10
	Nuvoco_RFQ_21-06-2021.exe	Get hash	malicious	Browse	• 103.124.93.155
	plan-536150726.xlsb	Get hash	malicious	Browse	• 103.28.39.29
	#U20ac9,770 pdf.exe	Get hash	malicious	Browse	• 103.28.36.229
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 103.57.209.110
	1400000004-arrival.exe	Get hash	malicious	Browse	• 103.28.36.198
	payment invoice.exe	Get hash	malicious	Browse	• 103.28.36.198
	Adjunto K_23165.doc	Get hash	malicious	Browse	• 103.28.39.103
	Adjunto K_23165.doc	Get hash	malicious	Browse	• 103.28.39.103
	211094.exe	Get hash	malicious	Browse	• 103.28.36.171
	PO20210120.exe	Get hash	malicious	Browse	• 103.124.93.25
	Electronic form.doc	Get hash	malicious	Browse	• 103.124.92.138
	SecuriteInfo.com.ArtemisC5924E341E9E.exe	Get hash	malicious	Browse	• 103.28.36.10
	Informacion 122020 N-98239.doc	Get hash	malicious	Browse	• 103.28.39.103
	INFO.doc	Get hash	malicious	Browse	• 103.28.39.103
	document-17616846.xls	Get hash	malicious	Browse	• 103.101.161.13
	document-17616846.xls	Get hash	malicious	Browse	• 103.101.161.13
	Information-822908953.doc	Get hash	malicious	Browse	• 103.101.162.60

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	djBbDPfGV3.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	CMXz729xzg.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	#Ud83d#Udcde_#U25b6Play_to_Listen.htm	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jssloader.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	gYbyE02c71.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	Copy of Check.html	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	diagram-1878769052.xls	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	statistic-1496367785.xls	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	Bank_ details.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	prijenos SWIFT za partiju 220000000001182910.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	PO29012021,pdf.ppam	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	OFfcxY5xia.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	k72fFnCoEX.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	DWJn18MuX6.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	sp7UUM849P.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	CL2SJ8-LYGF7Z-SEJ2QPPAPL.htm	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	AqZrR9upiM.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	iduD2A1.dll	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	E6973qZ1cV.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29
	97FC461FD24104740310BD741F7F8EBF489E640A A93A0.exe	Get hash	malicious	Browse	• 104.244.121.13 • 103.28.39.29

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\66988849-8D57-437E-97F2-4EBE1CC53C33	
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):	5.363066402926994
Encrypted:	false
SSDEEP:	1536:RcQIKNgeBTA3gBwlpQ9DQW+zoY34ZliKWXboOidX5E6LWME9:lEQ9DQW+zwXO1
MD5:	57CE0440BA2348963E599DB7CC6D4E70
SHA1:	9DC6386C0EFC19B9E88725D079F1561C74D3B672
SHA-256:	EF58DE4D929D2D78D172CFE4DCB94D8815D2447D6A7482670CC4E0CAB3C5283B
SHA-512:	B09ED0537E02581F7BF417E73D07A26F42AA40E2E7457D5E67FAA61033A653844939EA5FF6CEEA08158469A70F0690A92454F57523D8DE05A263CD6B78C1AE65
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="2021-06-29T22:08:25">.. 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\31DD4392.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	848

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\31DD4392.png	
Entropy (8bit):	7.595467031611744
Encrypted:	false
SSDEEP:	24:NLJZbn0jL5Q3H/hbqzej+0C3Yi6yyuq53q:JIjm3pQCLWYi67lc
MD5:	02DB1068B56D3FD907241C2F3240F849
SHA1:	58EC338C879DDBDF02265CBEFA9A2FB08C569D20
SHA-256:	D58FF94F5BB5D49236C138DC109CE83E82879D0D44BE387B0EA3773D908DD25F
SHA-512:	9057CE6FA62F83BB3F3EFAB2E5142ABC41190C08846B90492C37A51F07489F69EDA1D1CA6235C2C8510473E8EA443ECC5694E415AEAF3C7BD07F864212064678
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8O.T]H.Q..;3...?..fk.lR..R$.R.Pb.Q...B..OA..T$.hAD...J../..-h...fj..+....;s.vg.Zsw.=...{.w.s.w.@.....;..s...O..... ..;.y.p.....,...s1@ lr.:... .>.LLa..b?h...l.6..U....1....r.....T..O.d.KSA...7.YS..a.(F@....xe.^.I..$h....PpJ...k%.....9..QQ....h..!H*...../....2..J2..HG....A....Q&...k...d..&..Xa.t..E.. ..E..f2.d(..v.~.P.+.pik+;...xEU.g....._xfw...+...(..pQ.(..(.U./..)..@..?.....f.'...lx+@F...+....)..k.A2...r~B,....TZ..y..9...`..0....q....yY....Q.....A.....8j[.O9..t..&...g. I@ ..;..X!...9S.J5. .'.xh...8I.~.+...mf.m.W.i..{...+>P...Rh...+..br^$. q.^.....(..._.j...$..Ar...MZm|...9..E..!U[S.fDx7<....Wd.....p..C.....^MyI:...c.^..SI.mGj,.....!...h..$..;.....yD./..a...-j.^:.}..v....RQ Y*.^.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4A6A9A6B.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 246 x 108, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	10270
Entropy (8bit):	7.975714699744477
Encrypted:	false
SSDEEP:	192:3sXvKLMbye/PEXiKTUgCto9h4F6NwfU6vGDpdYNbcQZgkbd4cgc:3iLh/gJ59CDfU6LocbGK
MD5:	9C4F09E387EA7B36C8149EA7C5F8876E
SHA1:	FF83384288EB89964C3872367E43F25FAFF007CC
SHA-256:	A51C1D65092272DAEB2541D64A10539F0D04BC2F51B281C7A3296500CFCA56DE
SHA-512:	0FDDE22CFDDE8BB1C04842D2810D0FD6D42192594E0D6120DE401B08B7E2CFFB5333792BC748E93CD70FA14734CC7D950620CB977DDBBDB52D92BDA8F3552F8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....l.....sRGB.....pHYs.....+....'.IDATx^.].|.U...%...J."....H.&Ui.....E.....D.7....U.i..FH#=.....3..$K....'{3....7.....0.H.....H..03..,....8.q.....'@\. ..S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8..... .`..) @...X...q..>N...>.....q.....'@\...S@.../.0=....|....}|.....0.... ...,LO.....q._`az.....8...l..m.i'Sj.W.i.S.TJ....D.D._%...] ..i.;J..b..T.).Ik.L6..L.mN....!*..\..'{$.o._b..h....t"@.?...y...d..h..|..B9D..CJD..t."......bR"....I)H....z.....>|.....E.x..r....J.U..[...p:D....XF.....A...E.....b..C...C..C.....=.Z..$.=../....Y ..x5CY.0l..,~.W. .?.....;...$.'....<.H.2...z..6(.E.....kw8w^.\~...".C,gl&.m..J2.).HI.....b.r...'.....r.H...P....'...A.^.q..j).cZ.^1~.|.....dv^.^v..X..v..6/^.$rR. iK..H.Uu.Pvk....U.....'.Fd..Z .]mu*1.Zb.\b...N..P..&tr;.W....J.K(@.^A..R.S.[~.v.R.YO...0-...2..h."..............7..Ng...R...e.&..@..t..N...{5...W.x./#.%..}t...F8-..M1..(4b1....&.....)B...6.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\55637970.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 934 x 29, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	42557
Entropy (8bit):	**7.992800895943226**
Encrypted:	**true**
SSDEEP:	768:Pfsq4UmepRdblCFcXhw9KnRTRews6xD0FvBlwAS1A8x7BcS0OvD230:PR3ZblCF28KRsws6CFv0AYx7Bl3b230
MD5:	B1F262A694930ADB699FA94E3394887F
SHA1:	9C9B66D3A3F09AECA45DB94304CDD6FB3C5BD4C9
SHA-256:	9C99EC61392B9022A38C1354124360147E8185065095BD2EC92B1416CF9F4B68
SHA-512:	1CA7E6750178B88EC3AA7A0B83348EA389E26C27E0D7E919D807BE470714E5B4F04ACEB69D391F0498D4E465E6620E9449CA2F40755B5CE8196E683502EBF5F4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....6.....sRGB.....pHYs.....+.....IDATx^....dU....S.:ON.0.0....s0 .....$..%#HR.T.....$..0C...Su...[.TM..{.....C.S}..^{.....].^..ZX.Wb.W....X!..A.P... .0..u...X.V.3....z..tiO{GW..?...A.....ca2Y.... ...cAX..zZ..2M.$..g.O.e..r?z&.....*....*.=..Z.A.....a.Z..ka<..N.R.c...../.[..j.^...Nk.(..y.,..z"...R..Z+..D1Q....z....0..u~. .jU_.b.Z.V....:..5:..(.....-...A2.O.{..p.j..].<.....0..0..+...E...^...z....#..j.d...X._..1..M.5..O.^.."..I....G....U1.....X.6.Z.\.&..h..m*..T..xH.j..3<$.H...a..n....}t.A.jT.6G.h@..<.x..x...cb.. ....C..{.D.'QW<.o~..?.....4F_..B..h.\...y8..)....j.Z.d..#P..P..O.....(.0...f....B_z>.E .w../..(...'.Fw..yT..G..)...b9..g.AA`.a..v.zfY.F....._r.i.d.`....Q.g.m"..\..&.t.X.q1}.$.S....2..~...d."..1.. (.0.F....t...i..@f.. ...(..8..q.....I.....ad.....z%....;...y.O...X<Q..X.....B..H.....<)....4.&9.4.....1.h..#B.....g.....bO.59.A..M.....J..vX3*5..X....(G.A.u...8.. .{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6B5ED695.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 24 x 24, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	557
Entropy (8bit):	7.343009301479381
Encrypted:	false
SSDEEP:	12:6v/7aLMZ5l9TvSb5Lr6U7+uHK2yJtNJTNSB0qNMQCvGEvfvqVFsSq6ixPT3Zf:Ng8SdCU7+uqF20qNM1dvfSviNd
MD5:	A516B6CB784827C6BDE58BC9D341C1BD
SHA1:	9D602E7248E06FF639E6437A0A16EA7A4F9E6C73

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6B5ED695.png	
SHA-256:	EF8F7EDB6BA0B5ACEC64543A0AF1B133539FFD439F8324634C3F970112997074
SHA-512:	C297A61DA1D7E7F247E14D188C425D43184139991B15A5F932403EE68C356B01879B90B7F96D55B0C9B02F6B9BFAF4E915191683126183E49E668B6049048D35
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....o.....sRGB.....pHYs.....+.....IDAT8Oc.....l.9a._.X....@.`ddbc.].....O..m7.r0|..."......?A.....w..;.N1u....._.[.\Y...BK=...F +.t.M~..oX.. %....211o.q.P."......y...../..l.r...4..Q]..h.....LL.d.....d....w.>{.e..k.7.9y.%.. .YpI...{.+Kv...../..\[...A....^.5c..O?.....G...VB..4HWY...9NU...?..S..$..1..6.U.....c... ....7..J. "M..5. ...._.....d.V.W.c.....Y.A..S....~.C.....q.....t?..."n.....4.....G_.....Q..x..W.!L.a...3....MR.|.-P#P;..p._.....jUG....X.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D33DFFE4.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 521 x 246, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	32996
Entropy (8bit):	7.975478139053759
Encrypted:	false
SSDEEP:	768:N4k48AnTViUidx37OODgvnrxtxAudMN1VTRVHdB4K7K:NE8m+L37OOwrCXN1VTR1PK
MD5:	4E69B72B0CE87CC7EE30AA1A062147FE
SHA1:	09B0AA5414E08756E0AE53E1BE5C70DB4DEAF2E8
SHA-256:	77A1F749389CBF771D5197FF0FF17113FCA1D91989ADCADF2852876A6CC14988
SHA-512:	6246AF2137E773F7719033AFE75F0B00FF3A4B5543DBA53737FC8D33EE42478E3D8A5CF166E9EFD2F54A2F3E0D62417BDDC1CB824642305B59AB1229313D2D7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....[.J....sRGB.....pHYs.....+.....IDATx^.].`.....{%.$..A...R.P@z....O...S.<;.VT.REA.(...I...{.....m...]..r./.....~.|]h.Z....P.(.....E."@...P.(.v.P.@..E."@. ...#@y.....E."@y.....E."...*78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...)..... !@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3..P.(.....B.{..E.".y.P..ykNgL...P ..!@y.3.....E....."@...8C...g...).....!@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x...7x...S.(...g.P...!.=E."@..<.(o.5.3 ..P.(.....B.{..E.".y.P..ykNgL...P..!@y.3.....E....."@...8C...g...).....!@y..9.1E."@.p.....S.(....C....[s:c..E.".....!D...P.(.....t.....E....78C.~O...P.<....<o..).....3.(op...."@...x..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D45FCAB1.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 490 x 30, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	18547
Entropy (8bit):	7.9850486438978985
Encrypted:	false
SSDEEP:	384:kBCIQCloAwCZDy0xOTn6/g6l4NpWfw9nHk6Ka01f7Y/H:kBCIQpAwODPMT6/gfOUKN70
MD5:	ED31C7053D581EDC4C98D222CE02EDEF
SHA1:	6BA7A49CC6FF8FE00E9C5BC75F48AB7E679536DD
SHA-256:	0FCF61397154DF01CFAECA362BD643D88AAD5FEDD07B52DC8A921CC0D7236534
SHA-512:	929BF13F2A050B33D0EABDAC97CAAFDDE612AD521027FEE4DD51E28A3CF61198D6C045E00AB85223C73D74D18BB4EAA1681C7AFA917946DC08A3C75FB2AB4 935
Malicious:	false
Preview:	.PNG.....IHDR.....l{.....sRGB.....pHYs.....+....H.IDATx^...U....."x....U...."...Tc.{...M1M..In....TATb4F,`oD..Q..3.....g.3..Lr.D....a8....~.z....Z...yyF..9...:.H .Q2..)/L.....Q.}....(J.,...w2>R.$..G2..m>..\|...0.M.g.Xnjj...P.v..x....S.....B..p.=.Lz.^..Wi..2U.V'.a..*DE.'..rT.z....#.;..]....[?.C...o.m`]..m][;.:<..]F.9..u..Q]c.Ue.9....(.F.Z.~s..Q:..B.. .)..LZ.TTo..P.gc.l.'.X.}..H....Q.h\|....L..rcd.2dN..co..5.....w.U.4..}.....{.Q.....D2.J.z~..:Y3,.H..(#.J.Q.....N.._7....w.....].2w.6...._....u.....9-.7.f9...E9...p.A..f....=....Bqu....A .u.JG>b"...%..0..W.H=...G#.DR.....P.\|FD).NJ....)>.;...M...T*.dW..t:[.xT..M.\|S...O..."M.4u7.uS...]4..R.vK....*).ZK.. J.=.9C.].kr..ES..6..f.(.....N':..t..^.S....kn[s.#..(.....m.....~....6>.... :u.J.mO.....%D...Q...6%....!.....H.....v..^%....$._..V.....[o5.H8.....n.~M.z.RL.0p:.iC.k.1..$.....3[....mS5.....E...2.&...k]...A.....K.8...5..O.@7.[-.F4*7...i....in...y....A

C:\Users\user\AppData\Local\Temp\17B40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	160685
Entropy (8bit):	7.960590987645444
Encrypted:	false
SSDEEP:	3072:AL289VlUBWA6CFvA7brCxAVIKW1xVymd1xXPfZTkdm3bGeAxiYbX:/83liWA6FiYW1xVyWxffZTkeGKa
MD5:	7E75F03941F240AA7190A08B60F3DD64
SHA1:	D35A9AF59DE7669A5B834E47C8152434297A594F
SHA-256:	CD196E167E0BBC1054D6DA19E4D9392CC88A8DCE9FADF080E133350703B3318D
SHA-512:	8DD02F7956125D799B40A5EA3E26D985CEB9AC7D5B0415BC2EE93D1E23F421E6F81112B3F52B33FDF1541D03F805648C40438EA1F93EBC38C9BC3BE9C3D208 6
Malicious:	false

C:\Users\user\AppData\Local\Temp\17B40000	
Preview:	.U.n.0....?.....(..r.Mrl.$...\K....I..V.6P.....=H..pv.;.ZYS=AD.].....I...Z.....*L.)a.....:.V..e}J...({.....G+....!...~9.|.....)c.....fE..%s.X.u.].j...h)...ON."..b.%(/.-A7."..=@...Q.c....`..(gp.+Nm..>....q2....,G.^..@f...w..a..N..ZAu'b.&,..W.?...{.lv.d3-..`..Xc.....(..T".....#u\.':>.#.%.Cb..0.'g[.9.....G.....57..zz}..=vbZ..3...t.s/"..Dm.;.....PQ<g.|x8...h./.....p../.>G.. &...?.A..4.NN7.!.@.p.2.g?.....PK.....!..t.....[Content_Types].xml ...(..... ....

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$plan-515372324.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**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.950442215459519
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-515372324.xlsb
File size:	159199
MD5:	08e52afbefa423fb9f1ea0af88a4880e
SHA1:	2d688dfee28f75553bc1d3633f891d2e70e0408b
SHA256:	aaa32ff3e41c61fe828f0850e702f5ed7ffd6177c4bf80ed15324525537f44cd
SHA512:	7a5400ec826ecaa0fa6a8beb9022bd9e918f11cf97e57d747477720889f7203af983620e2f7b543fb1ff5cc5a9eff13447d6353506c862dfe2ebd23b7a63dee8
SSDEEP:	3072:q9VlUBWA6CFvA7bpKCxAVIKa8d/p4DqLdb1luxVymd1xXPtLrC/:q3liWA6FVNYa8dh4exQxVyWxfta
File Content Preview:	PK.....!.d/.}.....[Content_Types].xml ...(..... ....((..... .....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "plan-515372324.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 00:08:32.504199982 CEST	192.168.2.4	8.8.8.8	0x74e2	Standard query (0)	khangland.pro	A (IP address)	IN (0x0001)
Jun 30, 2021 00:08:34.005776882 CEST	192.168.2.4	8.8.8.8	0xc7a2	Standard query (0)	jaipurbynite.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 00:08:32.930166960 CEST	8.8.8.8	192.168.2.4	0x74e2	No error (0)	khangland.pro		103.28.39.29	A (IP address)	IN (0x0001)
Jun 30, 2021 00:08:34.156178951 CEST	8.8.8.8	192.168.2.4	0xc7a2	No error (0)	jaipurbynite.com		104.244.121.13	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

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 00:08:33.399928093 CEST	103.28.39.29	443	192.168.2.4	49739	CN=khangland.pro CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Jun 11 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Fri Sep 10 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		
Jun 30, 2021 00:08:34.565370083 CEST	104.244.121.13	443	192.168.2.4	49741	CN=jaipurbynite.com CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Mar 31 02:00:00 CEST 2021 Mon May 18 02:00:00 CEST 2015 Thu Jan 01 01:00:00 CET 2004	Wed Jun 30 01:59:59 CEST 2021 Sun May 18 01:59:59 CEST 2025 Mon Jan 01 00:59:59 CET 2029	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="cPanel, Inc. Certification Authority", O="cPanel, Inc.", L=Houston, ST=TX, C=US	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Mon May 18 02:00:00 CEST 2015	Sun May 18 01:59:59 CEST 2025		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6272 Parent PID: 800

General

Start time:	00:08:23
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:	0xba0000
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: splwow64.exe PID: 6156 Parent PID: 6272

General

Start time:	00:08:25
Start date:	30/06/2021
Path:	C:\Windows\splwow64.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\splwow64.exe 12288
Imagebase:	0x7ff6ec6a0000
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

Analysis Process: regsvr32.exe PID: 6464 Parent PID: 6272

General

Start time:	00:08:34
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\palpy1.dll
Imagebase:	0xd60000
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: 6672 Parent PID: 6272

General

Start time:	00:08:35
Start date:	30/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\palpy2.dll
Imagebase:	0xd60000
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