Joe Sandbox Cloud BASIC

ID: 432926
Sample Name: document-47-2637.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 23:38:13
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

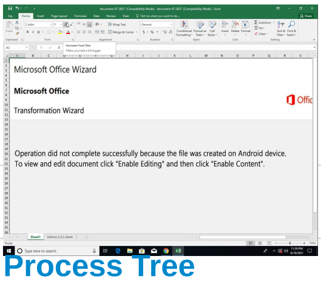
Analysis Report document-47-2637.xls

Overview

General Information

Sample Name:	document-47-2637.xls
Analysis ID:	432926
MD5:	92dcc47a1a044fc..
SHA1:	6f9266a6c0b702c..
SHA256:	ac4b99079b1ceb..
Tags:	xls
Infos:	

Most interesting Screenshot:



document-47-2637 [Compatibility Mode] - document-47-2637 [Compatibility Mode] - Excel

Microsoft Office Wizard

Microsoft Office

Transformation Wizard

Operation did not complete successfully because the file was created on Android device.
To view and edit document click "Enable Editing" and then click "Enable Content".

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

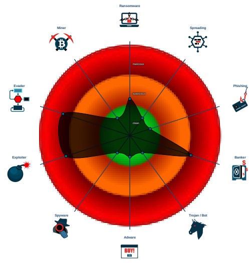
Hidden Macro 4.0

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

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Checks if browser processes are run…
- Contains functionality to compare us…
- 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…
- Allocates a big amount of memory (p…
- Binary contains a suspicious time st…
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6968 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - cmd.exe (PID: 7156 cmdline: 'C:\Windows\System32\cmd.exe' /c copy '%ProgramFiles(x86)%\Internet Explorer\ExtExport.exe' C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - nnAzot.exe (PID: 4600 cmdline: 'C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe' C:\aZ8ThU0Y\ERdZMUem GdPT AuMr7 MD5: CE639EB63B7C1C1EC94651B65CCEC383)
- **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)

E-Banking Fraud:

Checks if browser processes are running

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

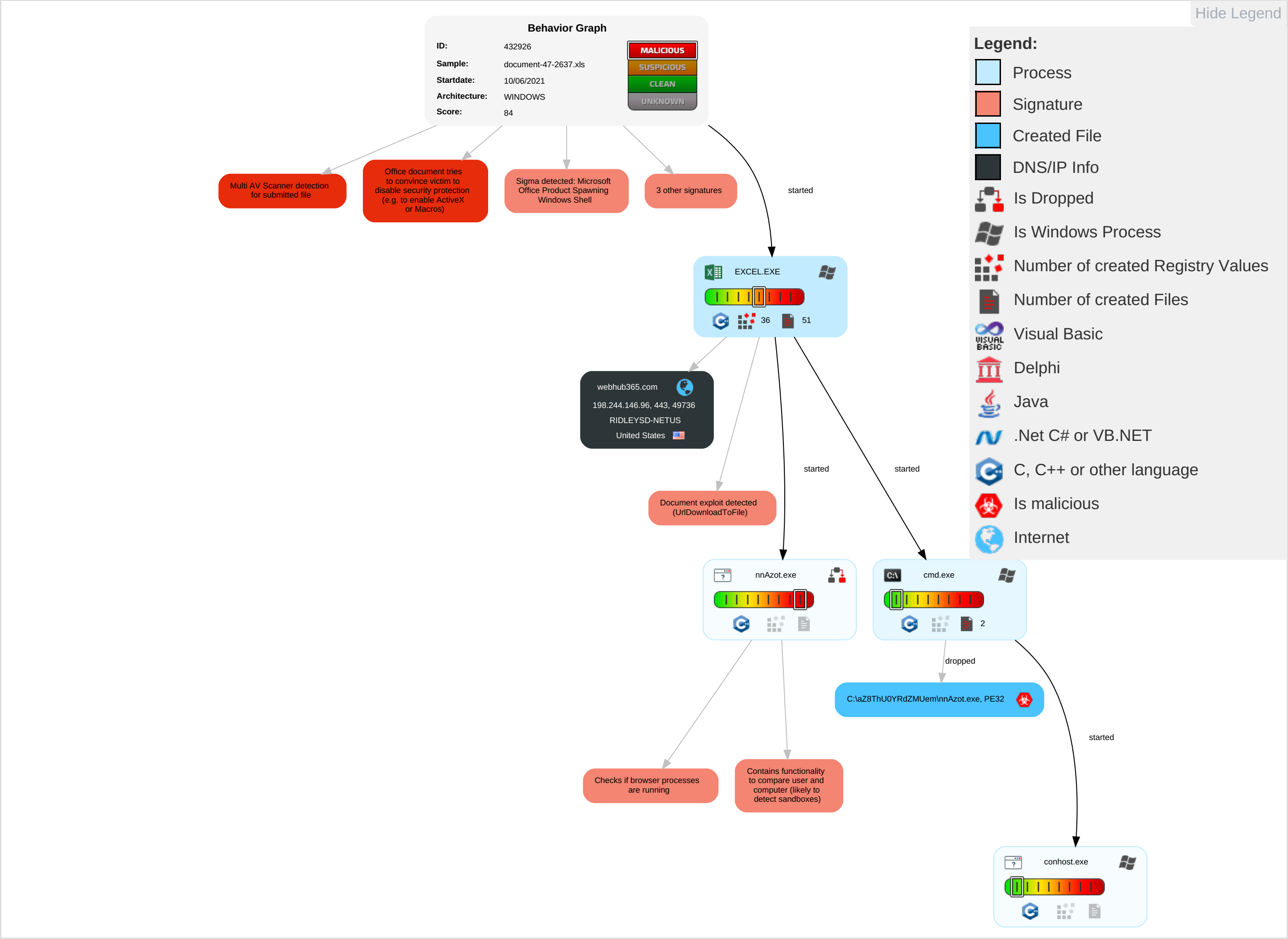
Malware Analysis System Evasion:

Contains functionality to compare user and computer (likely to detect sandboxes)

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	Application Shimming 1	Process Injection 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Application Shimming 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe D Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Process Injection 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

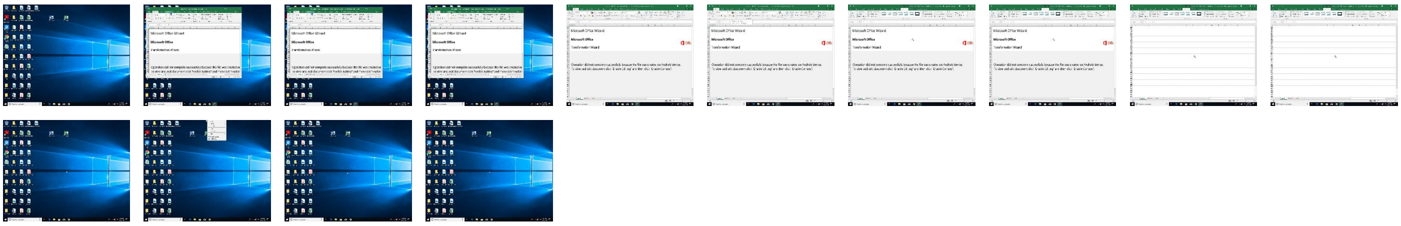
Behavior Graph

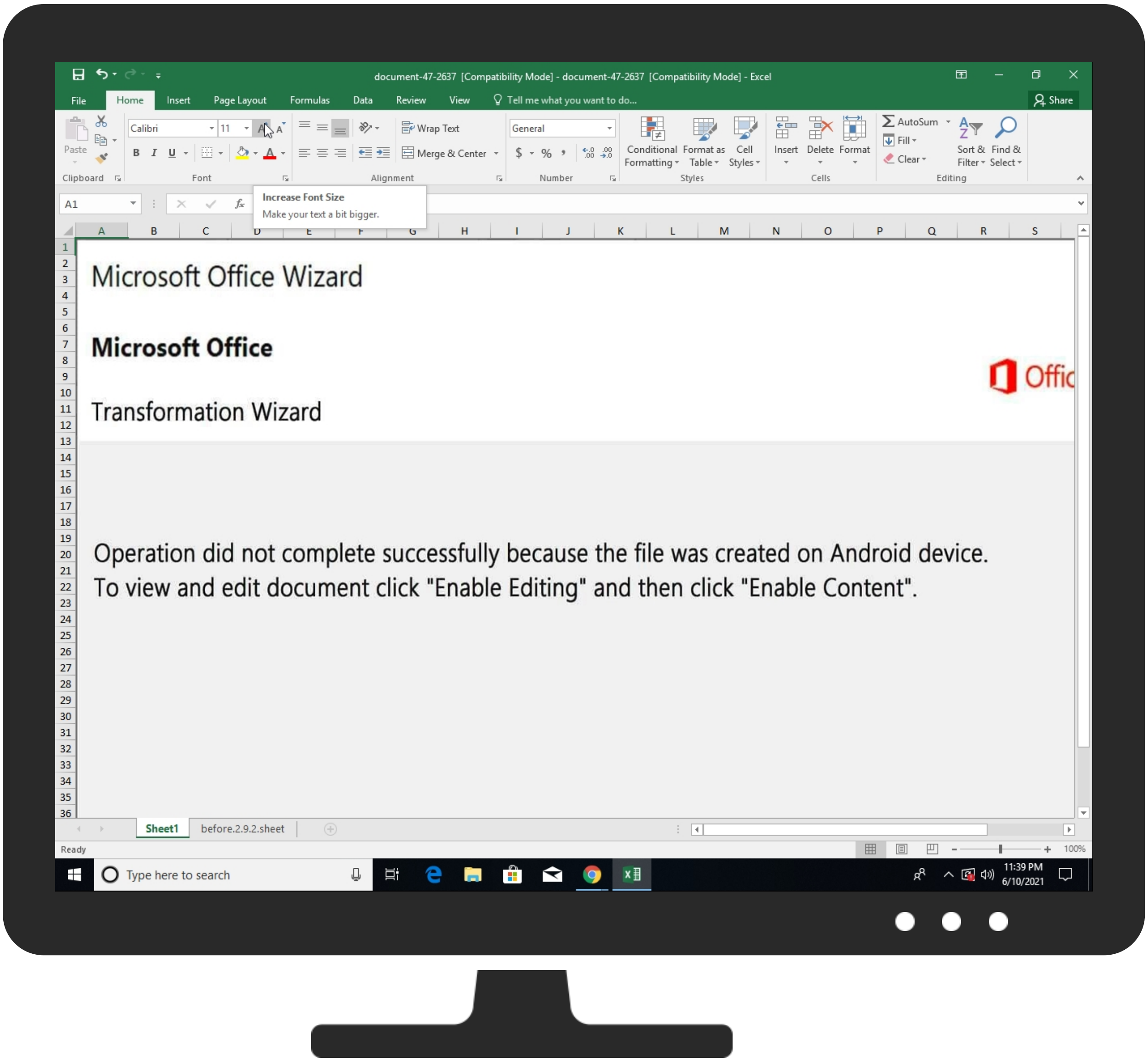

Behavior Graph
ID: 432926
Sample: document-47-2637.xls
Startdate: 10/06/2021
Architecture: WINDOWS
Score: 84
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Multi AV Scanner detection for submitted file
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)
Sigma detected: Microsoft Office Product Spawning Windows Shell
3 other signatures
started
EXCEL.EXE
36
51
webhub365.com
198.244.146.96, 443, 49736
RIDLEYSD-NETUS
United States
Document exploit detected (UrlDownloadToFile)
started
started
nnAzot.exe
cmd.exe
2
dropped
C:\aZ8ThU0YRdZMUem\nnAzot.exe, PE32
started
Checks if browser processes are running
Contains functionality to compare user and computer (likely to detect sandboxes)
conhost.exe
Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.




document-47-2637 [Compatibility Mode] - document-47-2637 [Compatibility Mode] - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Tell me what you want to do...
Share
Increase Font Size
Make your text a bit bigger.
Office
Sheet1
before.2.9.2.sheet
Ready
Type here to search
11:39 PM
6/10/2021

Microsoft Office Wizard

Microsoft Office

Transformation Wizard

Operation did not complete successfully because the file was created on Android device.
To view and edit document click "Enable Editing" and then click "Enable Content".

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
document-47-2637.xls	26%	Virustotal		Browse
document-47-2637.xls	23%	Metadefender		Browse
document-47-2637.xls	15%	ReversingLabs	Document-Office.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	0%	Metadefender		Browse
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
webhub365.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%	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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webhub365.com	198.244.146.96	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.244.146.96	webhub365.com	United States	🇺🇸	18630	RIDLEYSD-NETUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond

Analysis ID:	432926
Start date:	10.06.2021
Start time:	23:38:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	document-47-2637.xls
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:	19
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.bank.expl.evad.winXLS@6/9@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 86.3%) • Quality average: 69.6% • Quality standard deviation: 34.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • 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
198.244.146.96	document-47-2637.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RIDLEYSD-NETUS	document-47-2637.xls	Get hash	malicious	Browse	• 198.244.146.96

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Fax_Doc#01_5.html	Get hash	malicious	Browse	• 198.244.146.96
	wa71myDkbQ.exe	Get hash	malicious	Browse	• 198.244.146.96
	Current-Status-062021-81197.xlsb	Get hash	malicious	Browse	• 198.244.146.96
	logo.png.exe	Get hash	malicious	Browse	• 198.244.146.96
	3F97s4aQjB.xlsx	Get hash	malicious	Browse	• 198.244.146.96
	WcCEh3daIE.xls	Get hash	malicious	Browse	• 198.244.146.96
	ATT00005.htm	Get hash	malicious	Browse	• 198.244.146.96
	kxjeAvsg1v.exe	Get hash	malicious	Browse	• 198.244.146.96
	VSA75RUmYZ.exe	Get hash	malicious	Browse	• 198.244.146.96
	iX22xMeXIc.exe	Get hash	malicious	Browse	• 198.244.146.96
	QWkt5w3cO2.exe	Get hash	malicious	Browse	• 198.244.146.96
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 198.244.146.96
	vTtOheCXBQ.exe	Get hash	malicious	Browse	• 198.244.146.96
	6b6zVfqxbk.xlsb	Get hash	malicious	Browse	• 198.244.146.96
	Check 57549.Html	Get hash	malicious	Browse	• 198.244.146.96
	audit-78958169.xlsb	Get hash	malicious	Browse	• 198.244.146.96
	Docc.html	Get hash	malicious	Browse	• 198.244.146.96
	askinstall39.exe	Get hash	malicious	Browse	• 198.244.146.96
	Lista e porosive.exe	Get hash	malicious	Browse	• 198.244.146.96
	askinstall39.exe	Get hash	malicious	Browse	• 198.244.146.96

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	document-37-1849.xls	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\9C265DD6-ED91-4AAE-9C37-56E57236292F

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):	134922
Entropy (8bit):	5.369107251625446
Encrypted:	false
SSDEEP:	1536:KcQIKNEeBXA3gBwlpQ9DQW+z7534ZliKWXboOilX5ENLWME9:aEQ9DQW+ziXOe
MD5:	4885913667B0E212E6E83C9B74AF771A
SHA1:	EFFDDE591047639F3DCF4034807D9F37A35426FE
SHA-256:	59756C811635EBF4C1F1794D57FC4A758E1A7A93DA0F74FDCC66C1C83AE0ABAC
SHA-512:	ACF822176355AAFEF2A04265976B9BC65BCEC067604B359FD50B468112E85B7EB68BA17BF1EAC626D7F78B08DE190D0CE6474136F9DDF84A9BA2F2B39C245D 5
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="2021-06-10T21:39:04">.. Build: 16.0.14209.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Temp\3FA40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	68601
Entropy (8bit):	7.6095013473066455
Encrypted:	false
SSDEEP:	768:5X3vegIg9kOKLUwxZi4IB5/vAVk/ViuHpc2HoM3DFZXHHHHHHHHHLGAX4MOw+j8j:rkNLPHqvAk/Vi6+YDT7Hbc8hxCCVl/
MD5:	9F3996ECBC98180FD2BCFE840C41E4CA
SHA1:	30F402A14E8F22F3E9B72DA06E2419537E511281

C:\Users\user\AppData\Local\Temp\3FA40000

SHA-256:	CCA5AA32910672FE42CB13FF0207E8E15602E3FF67D3C29044221C8718331128
SHA-512:	7B3BFD8DD34674EC9E988A5EDB4FB4C5028C72C6862A634BE362A56F6F86AAD3799FFA4FB088649EC24CFE57188A1CF7E5C16BD17B1FAC599146C05369797A9 A
Malicious:	false
Reputation:	low
Preview:	.TKo.0.....0t.l.;.....>.].u?...X.^..6....4} .W..[6.=H.....m.1......D4.U../z....)...5...k$q>.v2.[G...z1...IIj@....#..d.L..A-a...dr&U..}ns....%.....j.7N.E\..b..h..BP.r/&...........^.p.n]u..{h0...u._.D.z+....r&.....o..u...)..}...0Iq..B...;.*.+...9..8<.T.$...?$..Y..s.P.....:..AW2g..I]....?kd..+zD&.CY..gZiF.).-...uC:.<@B."n./7.{.N.T,.....o....m.M!.......K..t...S6...}..S..?....7.z....t........PK.........!...<...........[Content_Types].xml ...(...MO.0...H.......BKwAH.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Thu Jun 10 20:39:07 2021, atime=Thu Jun 10 20:39:06 2021, length=12288, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.672568751401007
Encrypted:	false
SSDEEP:	12:8oSCXUVduCH2KOeLR4miS68+WrjAZ/DYbDJp5SeuSeL44t2Y+xIBjKZm:85i1S1AZbcDJpP7aB6m
MD5:	CB5861A7C65B698B00B963BDB3A65EAE
SHA1:	30BD2B243AA0913959069D2B7E81E0631BCE55B7
SHA-256:	11D2C94BA62AD8C8224DC0C70E330801DA0020DE457F2180FF905886F5EE79A9
SHA-512:	632645EBBCB2F6B0CE3F46EF41DC8CD4E71AD18704BE52E47B33CE5B0F94C89053BD3A4BDAFBFBDF68A48F8BAB4952A725FEC40CBBE21025F551D49086AB4 D3A
Malicious:	false
Reputation:	low
Preview:	L..................F.............-....U.A^...%Q.A^...0......................u....P.O. .:i.....+00.../C:\..................x.1......N....Users.d......L...R....................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.......N...R.....#J.....................Z.j.o.n.e.s.....~.1......R...Desktop.h.......N...R......Y.............>.....v..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.......E...............-.......D...........>.S......C:\Users\user\Desktop.......\.....\.....\.....\.....\.D.e.s.k.t.o.p.........:..,.LB.)...As...`.......X.......123716...........!a..%.H.VZAj...m<..............!a..%.H.VZAj...m<.........................1SPS.XF.L8C....&.m.q.........../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.........9...1SPS..mD..pH.H@..=x.....h....H......K*..@.A..7sFJ...........

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\document-47-2637.LNK

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:53 2020, mtime=Thu Jun 10 20:39:07 2021, atime=Thu Jun 10 20:39:07 2021, length=92672, window=hide
Category:	dropped
Size (bytes):	2170
Entropy (8bit):	4.721481944923777
Encrypted:	false
SSDEEP:	24:8MyEmiQGNAobv1DJpf7aB6myMyEmiQGNAobv1DJpf7aB6m:8Mgi1Go7PQB6pMgi1Go7PQB6
MD5:	5940923A2A431724DABE37F3633871D0
SHA1:	2509A2D6150538B6B238C22023F6A4C1CAD3BCF6
SHA-256:	AD29413158F192C2C3425D01B987D4B547FC1F2CE05F1C97AF92962DB2F5279B
SHA-512:	481B7908EFDD5174A8FBA30AD8AC57D77F2789DBEEE832EBA99CF834A515E189DF36E5260442671E28088A0C91668D82A25BBDB936E467163BF5C2355B08772
Malicious:	false
Reputation:	low
Preview:	L..................F.... ...ig.S....W.Z.A^..W.Z.A^...j..........................P.O. .:i.....+00.../C:\..................x.1......N....Users.d......L...R....................:......;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q|<..user.<.......N...R.....#J.....................Z.j.o.n.e.s.....~.1.....>Q}<..Desktop.h.......N...R......Y.............>.......1.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....v.2..h...R. .DOCUME~1.XLS..Z......>Q{<.R......V.....................m..d.o.c.u.m.e.n.t.-.4.7.-.2.6.3.7...x.l.s.......Z...............-.......Y...........>.S......C:\Users\user\Desktop\document-47-2637.xls..+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.o.c.u.m.e.n.t.-.4.7.-.2.6.3.7...x.l.s.........:..,.LB.)...As...`.......X.......123716...........!a..%.H.VZAj...................!a..%.H.VZAj.............................1SPS.XF.L8C....&.m.q.........../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.781102818999889
Encrypted:	false
SSDEEP:	3:oyBVomMY9LRkKSd6YCZELRkKSd6YCmMY9LRkKSd6YCv:dj6Y9LaJdzgELaJdzUY9LaJdzs
MD5:	CC574425794FB97F59C2DC249939493A
SHA1:	8CA2DFD4C2535E0FFEB160319D2CD079758B7F8D
SHA-256:	1D977854F9C0DDF7462B6991CA2B6026C4FFCAF52F158A2C7B81B8FBEE5E35F0
SHA-512:	6C9C7CAFA742354DB174653D4C1CF9521AC10C67177FB2E26A85AE1267F1A45094BD1F1AE3C0B53836D5210F6083906F17C26A28A197D0CCF2F76D7447272E4
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Reputation:	low
Preview:	Desktop.LNK=0..[xls]..document-47-2637.LNK=0..document-47-2637.LNK=0..[xls]..document-47-2637.LNK=0..

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:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\00B40000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	dropped
Size (bytes):	117445
Entropy (8bit):	7.924149420001192
Encrypted:	false
SSDEEP:	3072:UfgagkFMp1lsZaVV6zBiA2AiuLKli2LKefgag2:0xFCLPVV+BiA2Ai0uicDd
MD5:	40F42EC6AF84151ABC504FB591A42BD4
SHA1:	13504B444A7127A12C99F75D389D8BE78F607811
SHA-256:	4342F4D6263F70D2BEC42C6D8CC1E6F23811C416265FBBF688D8D2F1AA2C5BFF
SHA-512:	52B8B4DACF29DDA70A1C63FA16F7B6D9363DC852FC9D2C4BD381DBB8C6694A131CD5D19697B45293BD5E07CA399A422EED48FDD48D7B0177C1398086F9344 1
Malicious:	false
Reputation:	low
Preview:	........T8........../.............+.F|..14.l.0..e.i...t...y...$......O~..m.........T8........../.6...........+.F\|..14.l.0..e.i...t...y...$......O~..m............f....\.p...'...0...u.........0.... d..o3......+...#uN'.wd.. ^.J.9v!..z.+....+k,l.%<....>t...'..........h...T:.x..5..B.....a....j....=....]......O.....6.................!....Nr=.......1.[...9.F^....@.........]."....................^1...V...D?..vQ.....Y...........O.1......(G.Z.!. AP[..:=9.LY;....~].1....{.t.D9..j...y..z.`t.......;.1...[sN5..)......2.H\........k....1.....4=(R...x.......`.0.,..g.61.*.B.y/.v\.2^<..[!.1......Y..........O.O..(.1......*)..U.c-..3.nxt"..l...p1....w!0..@....].* ....:s.,|O.T.>1.....4L.0{....s.e.h.)}....O.$}.1...'.OA<Z.....E...K....._xL...1....L...[..j.qm..^..1...O....a#.1.....!...^..(.1.FP.;...........1....dK.;.....B.r....wb....9.b.1...=..i.x.Q.x:.....(./.. L^..1...... >Z..I.....Z.s...x[.}..vX..1...5..}%.gY...$.....:.....'1..R.1....JX!............c.3.,.*.m+..5.1...

C:\Users\user\Desktop\4F850000

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Applesoft BASIC program data, first line number 16
Category:	modified
Size (bytes):	99740
Entropy (8bit):	7.929925379753235
Encrypted:	false
SSDEEP:	1536:n6hF9uwbh8+yV1jngo7mfk9mjhjAefouRA+VkV43RBVCOG6hFouT:nWuihUJngIQjAehZVkqbsjuT
MD5:	BA34233274FF56530F9141B9F5B5FF43
SHA1:	974F24CCD4BEE89423AF7B4ABB09537605AFD1A3
SHA-256:	D79872EFE978946ADD8D6DD0848835F0A365B69F588C0FA52F744B88FC1D10F7
SHA-512:	A27822A9DE321CE36E0BA71AEF683CCF429F43B9DBA216E086EBF186A8A037AE2DA45C0E97CCA5F6C240FE43DF173668DCA673CA6957F371C8BA42653461B8 FF
Malicious:	false
Reputation:	low
Preview:	........T8........../...........X.-...f..7.........E..54...rI.89B\."......Q+........T8........../.6.........X.-...f..7.........E..54...rI.89B\."......Q+..........ut....\.p.!...8em.....W..4.W?..[S`..L.b%A...sH/.#. ;.*8.Z..^.'.y..;."C["....mE....g...o_../T...h4)N.g..6....`...^MJ..#B.....a.........=...........&....9w....Gh.....f..........zT=....a.5..i...u.y.i@.........."..........g.....Y.....\1.....S.b2#J...A.k.t..\.?P.tx.. .o.1...]...k..U.-.).%4.@a...*/..D..1... ~v....^|]..4.2b....x..3..1....uR....Z.A.T..=..Q.J."[.*Lf..1....u....NR....!.-..-.".8.uH7.XQ~1.*.x'..v..lU.*c\...s..O.'l.0...{.".2:...j<6w1.....DI....R.T..5.K... .X.|5..C<..1....A@..."..|....r.$6T..(Hk[v3&|.1......{.=.P.Od.QY.....S.....^`..1....W8.[..?K..'.)..(...Q..}1..... ....g.H...1....r.....',..1....*.2.Z..\..jw.w.."..".."..Yu.0K.1.........l'%...,..z.L../N@>. C.~bW1........G.._.e.7|.g.c:c.Y='....,1......1.....p^.7d}.@(.....&....1....M..t.d.".p^[+.k.2...;..b...1.....DQ q...,i...G_.[3.|.7....1...

C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows

C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe	
Category:	dropped
Size (bytes):	44544
Entropy (8bit):	6.190125674423799
Encrypted:	false
SSDEEP:	768:AAMBmP3+XxLKZ/XMsQt1TZPImKXPXtE6MayeDkX0PmfkPchaDPfsRi7P4QG64iuU:UsP3+XxLKZ/XMsQt1TZPImKXPdfDkXSZ
MD5:	CE639EB63B7C1C1EC94651B65CCEC383
SHA1:	B92544ED405C33F2DB64A0BCA41646CB712E246B
SHA-256:	2D2EAD13B2796AD58D070DC1FD36961866F25E1E436661C760A879EAC35982F9
SHA-512:	66E841C9DF0D17AB1A1C866A96769AD0F4F8329C94EDB2917648FB4FF76E7A47C479A60A0D05293136843EC5BA938B0CEB96190BEE01AE049A467BDA45CB456 6
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: document-37-1849.xls, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......h.\D,.2.,.2.,.2.C.1.(.2.C.6.9.2.C.7./.2.C.3.=.2.,.3...2.C.;.:.2.C...-.2. C.0.-.2.Rich,.2.........PE..L.....]......................*......@.............@..@...... ....+..T.. ....text.............................. ..`.data...h..........................@....idata.............................@..@.rsrc..............................@..@.reloc.............................@..B.................. ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Windows User, Last Saved By: Windows User, Name of Creating Application: Microsoft Excel, Create Time/Date: Wed Jun 2 14:40:34 2021, Last Saved Ti me/Date: Wed Jun 2 14:40:36 2021, Security: 1
Entropy (8bit):	7.59086745125602
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	document-47-2637.xls
File size:	92165
MD5:	92dcc47a1a044fc3a2328ec6eef3918b
SHA1:	6f9266a6c0b702cbaa0a3583df5c8cd1357eae35
SHA256:	ac4b99079b1ceb11db593097e421de9d9092765feedc23 a3ab8ef912b292c988
SHA512:	fcd4b7c0a4e0f785604f40e0a9a4690e9b642223ee63088 c6c4acfc262a18f5a79c77ab82498b422b229eaecc9a2e7 45b7e455c43ad2a85794e7adbac6b9bafd
SSDEEP:	1536:Lc2ZSmXWCQnp2c90Hg+j8z3kVfKIDVzoFGUslI B54N+wl8MYBzaVt4J5aukGqu:LXZxXTQ8hHgNQNeF3 V4NvuhBzaV+J5a+
File Content Preview:	........................>.. ....

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "document-47-2637.xls"

Indicators

Has Summary Info:	True

Indicators

Application Name:	Microsoft Excel
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1252
Author:	Windows User
Last Saved By:	Windows User
Create Time:	2021-06-02 13:40:34
Last Saved Time:	2021-06-02 13:40:36
Creating Application:	Microsoft Excel
Security:	1

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams

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 10, 2021 23:39:07.696746111 CEST	192.168.2.4	8.8.8.8	0x412	Standard query (0)	webhub365.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 23:39:07.756989002 CEST	8.8.8.8	192.168.2.4	0x412	No error (0)	webhub365.com		198.244.146.96	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 10, 2021 23:39:07.875941038 CEST	198.244.146.96	443	192.168.2.4	49736	CN=webhub365.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.	Tue Jun 08 19:53:43 CEST 2021 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Mon Sep 06 19:53:43 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: 6968 Parent PID: 800

General

Start time:	23:39:03
Start date:	10/06/2021
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:	0xfd0000
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 7156 Parent PID: 6968

General

Start time:	23:39:08
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c copy '%ProgramFiles(x86)%\Internet Explorer\Ext Export.exe' C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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 Written

File Read

Analysis Process: conhost.exe PID: 6172 Parent PID: 7156

General

Start time:	23:39:08
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: nnAzot.exe PID: 4600 Parent PID: 6968

General

Start time:	23:39:10
Start date:	10/06/2021
Path:	C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe

Wow64 process (32bit):	true
Commandline:	'C:\aZ8ThU0Y\ERdZMUem\nnAzot.exe' C:\aZ8ThU0Y\ERdZMUem GdPT AuMr7
Imagebase:	0x1150000
File size:	44544 bytes
MD5 hash:	CE639EB63B7C1C1EC94651B65CCEC383
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis