

JOeSandbox Cloud BASIC



ID: 648583

Sample Name:
WF0SIQWkr1.docx

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 08:17:06

Date: 20/06/2022

Version: 35.0.0 Citrine

Table of Contents

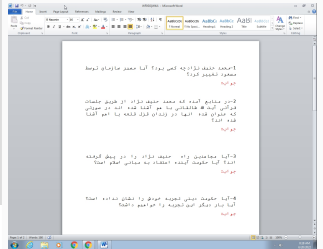
| | |
|--|----|
| Table of Contents | 2 |
| Windows Analysis Report WF0SIQWKr1.docx | 3 |
| Overview | 3 |
| General Information | 3 |
| Detection | 3 |
| Signatures | 3 |
| Classification | 3 |
| Process Tree | 3 |
| Malware Configuration | 3 |
| Yara Signatures | 3 |
| Initial Sample | 3 |
| Sigma Signatures | 3 |
| Snort Signatures | 4 |
| Joe Sandbox Signatures | 4 |
| AV Detection | 4 |
| System Summary | 4 |
| Mitre Att&ck Matrix | 4 |
| Behavior Graph | 4 |
| Screenshots | 5 |
| Thumbnails | 5 |
| Antivirus, Machine Learning and Genetic Malware Detection | 6 |
| Initial Sample | 6 |
| Dropped Files | 6 |
| Unpacked PE Files | 6 |
| Domains | 6 |
| URLs | 6 |
| Domains and IPs | 7 |
| Contacted Domains | 7 |
| World Map of Contacted IPs | 7 |
| General Information | 7 |
| Warnings | 7 |
| Simulations | 7 |
| Behavior and APIs | 7 |
| Joe Sandbox View / Context | 8 |
| IPs | 8 |
| Domains | 8 |
| ASNs | 8 |
| JA3 Fingerprints | 8 |
| Dropped Files | 8 |
| Created / dropped Files | 8 |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{42C9F637-8755-4609-AD1A-8AEF5BB0ED5D}.tmp | 8 |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7A315592-6D7F-4514-92E8-A3FEF3FF12EF}.tmp | 8 |
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DA250572-DF73-4B44-A755-D2E189FAE1C6}.tmp | 9 |
| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\WF0SIQWKr1.LNK | 9 |
| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | 9 |
| C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm | 10 |
| C:\Users\user\Desktop\~\$0SIQWKr1.docx | 10 |
| Static File Info | 10 |
| General | 10 |
| File Icon | 11 |
| Network Behavior | 11 |
| Statistics | 11 |
| System Behavior | 11 |
| Analysis Process: WINWORD.EXEPID: 1008, Parent PID: 576 | 11 |
| General | 11 |
| File Activities | 11 |
| File Created | 11 |
| File Deleted | 11 |
| File Read | 11 |
| Registry Activities | 12 |
| Key Created | 12 |
| Key Value Created | 12 |
| Key Value Modified | 13 |
| Disassembly | 16 |

Windows Analysis Report

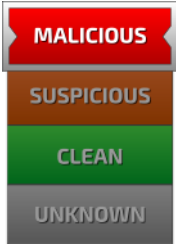
WF0SIQWkr1.docx

Overview

General Information

| | |
|--|-----------------------------|
| Sample Name: | WF0SIQWkr1.docx |
| Analysis ID: | 648583 |
| MD5: | 783f850d06c9f12.. |
| SHA1: | 08011884c9bed1.. |
| SHA256: | 211a1f74eea68e.. |
| Tags: | CVE-2022-30190 docx Follina |
| Infos: | Yara |
|  | |

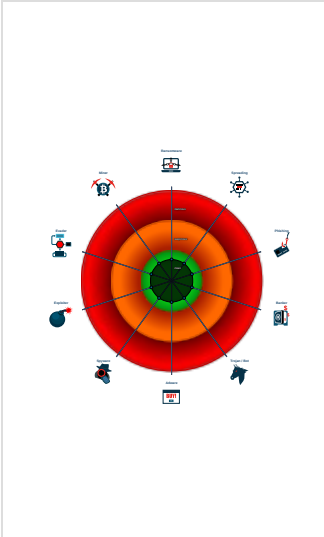
Detection

| | |
|---|---------|
|  | |
| Score: | 56 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

Signatures

| |
|--|
| Malicious sample detected (through... |
| Multi AV Scanner detection for subm... |
| Yara signature match |
| Document misses a certain OLE str... |

Classification



Process Tree

- System is w7x64
-  WINWORD.EXE (PID: 1008 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- cleanup

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

| Source | Rule | Description | Author | Strings |
|-------------------|------------------------------|--|-----------|--|
| document.xml.rels | INDICATOR_OLE_RemoteTemplate | Detects XML relations where an OLE object is referencing an external target in dropper OOXML documents | ditekSHen | <ul style="list-style-type: none">0x38a:\$olerel: relationships/oleObject0x3a3:\$target1: Target="http0x3df:\$mode: TargetMode="External |

Sigma Signatures

No Sigma rule has matched

Snort Signatures

 No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

System Summary



Malicious sample detected (through community Yara rule)

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 | Impact |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|---|-----------------------|---|-------------------------|---------------------------|--|--|---|---|-------------------------|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Path Interception | <div>1</div> Masquerading | OS Credential Dumping | <div>1</div> File and Directory Discovery | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | <div>1</div> Ingress Tool Transfer | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | <div>1</div> System Information Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |

Behavior Graph

Behavior Graph

ID:

648583

Sample:

WF0SIQWkr1.docx

Startdate:

20/06/2022

Architecture:

WINDOWS



Score:


56




- Legend:
- Process
 - Signature
 - Created File
 - DNS/IP Info
 - Is Dropped
 - Is Windows Process
 - Number of created Registry Values
 - Number of created Files
 - Visual Basic
 - Delphi
 - Java
 - .Net C# or VB.NET
 - C, C++ or other language
 - Is malicious
 - Internet

Malicious sample detected
(through community Yara rule)

Multi AV Scanner detection
for submitted file

 WINWORD.EXE 

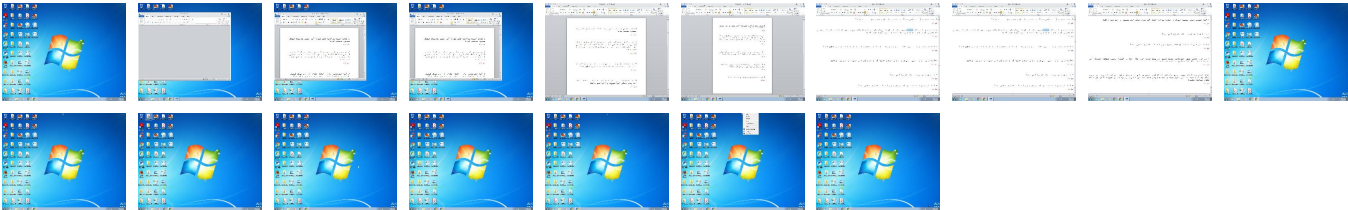


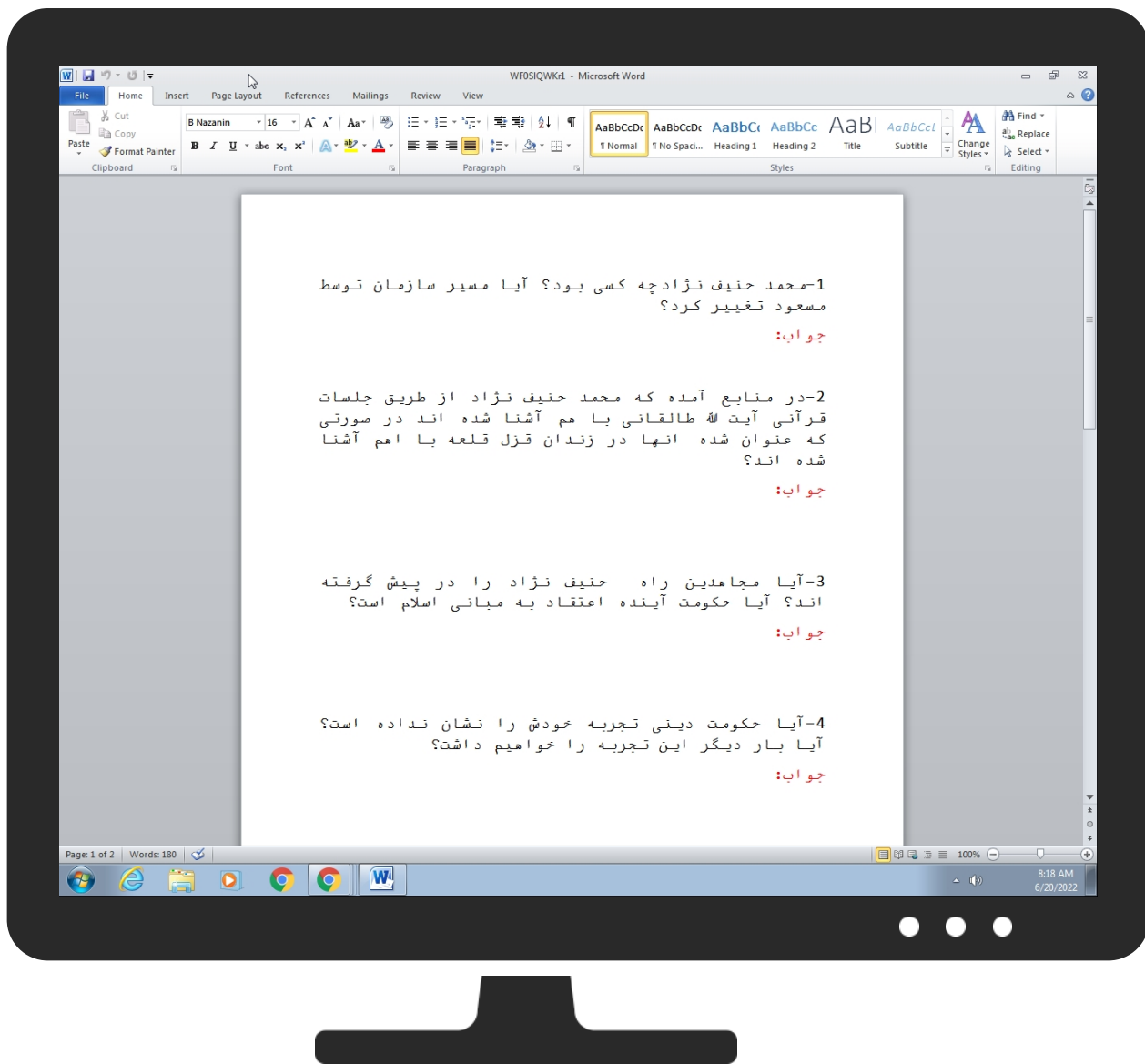
  502  22

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 |
|-----------------|-----------|------------|-------|------------------------|
| WF0SIQWkr1.docx | 20% | Virustotal | | Browse |

Dropped Files

⊘ No Antivirus matches

Unpacked PE Files

⊘ No Antivirus matches

Domains

⊘ No Antivirus matches

URLs

⊘ No Antivirus matches

Domains and IPs

Contacted Domains

 No contacted domains info

World Map of Contacted IPs

 No contacted IP infos

General Information

| | |
|--|--|
| Joe Sandbox Version: | 35.0.0 Citrine |
| Analysis ID: | 648583 |
| Start date and time: 20/06/2022 08:17:06 | 2022-06-20 08:17:06 +02:00 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 11m 10s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | WF0SIQWKr1.docx |
| Cookbook file name: | defaultwindowsofficecookbook.jbs |
| Analysis system description: | Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2) |
| Number of analysed new started processes analysed: | 2 |
| 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: | <ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal56.winDOCX@1/7@0/0 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | <ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0 |
| Cookbook Comments: | <ul style="list-style-type: none">• Found application associated with file extension: .docx• Adjust boot time• Enable AMSI• Found Word or Excel or PowerPoint or XPS Viewer• Attach to Office via COM• Scroll down• Close Viewer |


Warnings


- Max analysis timeout: 600s exceeded, the analysis took too long
- Exclude process from analysis (whitelisted): dllhost.exe
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetValueKey calls found.


Simulations


Behavior and APIs


 No simulations

| Joe Sandbox View / Context | |
|---|------------|
| IPs | |
|  | No context |

| Domains | |
|---|------------|
|  | No context |

| ASNs | |
|---|------------|
|  | No context |

| JA3 Fingerprints | |
|---|------------|
|  | No context |

| Dropped Files | |
|---|------------|
|  | No context |

| Created / dropped Files | |
|--|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{42C9F637-8755-4609-AD1A-8AEF5BB0ED5D}.tmp | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | Composite Document File V2 Document, Cannot read section info |
| Category: | dropped |
| Size (bytes): | 2560 |
| Entropy (8bit): | 1.4226238273348333 |
| Encrypted: | false |
| SSDEEP: | 12:rl3ITpFQojNIPv4Pv4CIPv4Pv4CICICb77:rmAuA |
| MD5: | D2A324F48794DD09E917A4733BDB17FC |
| SHA1: | E805061D7804CCB9F42DEC8769BCF8D7FE559637 |
| SHA-256: | 2461E1B86BF8005871695EC22328A322D4B56C6F37A4AF77D95A1CA83577D077 |
| SHA-512: | 850E3DC7ABAF0250BFF07E4F671091E88190FBAB2CE345F0C2AFC7C58A61D04F0323DC2959BF5AA0BDCDB22C4C0981127E52E2E1892B34C2D7DB3D4A3C7ECA8 |
| Malicious: | false |
| Reputation: | low |
| Preview: |>..... |

| | |
|--|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7A315592-6D7F-4514-92E8-A3FEF3FF12EF}.tmp | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 5340 |
| Entropy (8bit): | 4.345212231669781 |
| Encrypted: | false |
| SSDEEP: | 48:2KYZsXTdv9+UFi90cRaXqhi/hFo4EblZnVs85HnOojH10+3P1mVZTUGeb7:2YNg0VXqMZfKdnVdnO4C+yZTRg7 |
| MD5: | 2F8E2D63B388B0BB1EEEEFEACA5C6448E |
| SHA1: | 453512E99A2B353E57E3B41214F582379ADC32E3 |
| SHA-256: | DC6B2202014ECE613B5A51730D9CDEC2FD5AE3C34DC4751956D2CCB70F05BF8E |

| | |
|-------------|--|
| SHA-512: | FC4338047618650018DAFCA28AA186C7134834D068EAEB08EEB14649C4B85A0344E5A1C08093D73AB1C079DFB3F6F87D691EE6DE64FD87A04E6945A539E9DDf9 |
| Malicious: | false |
| Reputation: | low |
| Preview: | ..1.-E.-E./.-F...A..F.../...G...3... (H./... "..." .E3...1..3.'2.E.'F..*H.3.7..E.3.9.H./.*.....1...1/.....H.'(.....2-./1..E.F.'(9.."E./G...G..E.-E./.-F...A..F.../..'.2..7.1...B...D.3.'*..B.1".F... "...".'D.D.G..7.'D.B.'F... (.'..G.E.."4.F'.4./G..'/F./..1..5.H.1*...G..9.F.H.'F..4./G...'.F.G'./1..2.F./'F..B.2.D..B.D.9.G..(.'..G.E.."4.F'.4./G..'.F./.....H.'(.....3--"...'..E...'.G./...F.....Z...f...h...j.....\$.....A\$a\$.gd.z.....\$.....A\$a\$.gd...\$.....A\$a\$.gdH....\$. \$.....A\$a\$.gd.K.....\$.....A\$a\$.gd.....\$.....A\$a\$.gd2N..... |

| | |
|---|---|
| C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{DA250572-DF73-4B44-A755-D2E189FAE1C6}.tmp | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1024 |
| Entropy (8bit): | 0.05390218305374581 |
| Encrypted: | false |
| SSDEEP: | 3:ol3Ydn:4Wn |
| MD5: | 5D4D94EE7E06BBB0AF9584119797B23A |
| SHA1: | DBB111419C704F116EFA8E72471DD83E86E49677 |
| SHA-256: | 4826C0D860AF884D3343CA6460B0006A7A2CE7DBC4D743208585D997CC5FD1 |
| SHA-512: | 95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4 |
| Malicious: | false |
| Reputation: | high, very likely benign file |
| Preview: | |

| | |
|---|--|
| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\WF0SLQWkr1.LNK | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime= Tue Mar 8 15:45:52 2022, mtime= Tue Mar 8 15:45:52 2022, atime= Mon Jun 20 14:18:10 2022, length=12519, window=hide |
| Category: | dropped |
| Size (bytes): | 1019 |
| Entropy (8bit): | 4.53966222663807 |
| Encrypted: | false |
| SSDEEP: | 24:8VRnIBk/XTm3xqus/xfVQNe9yDv3qSAY7h:8Vxvk/XTQx6xfuNgh2h |
| MD5: | 1E38264369A659D7EBD3F43103830323 |
| SHA1: | 4DD713DAE522AF51DF0E3EF71AAB07F2D64919F8 |
| SHA-256: | A57F4711234DCAA5C508417C2C94EC9CC3683E731727BBB9DD523E806D661318 |
| SHA-512: | 35A562C15A30A72B852AB56C79EF302923D70157D136B0F827EAEFFFA579393902A2DBB7CD5CDFE3C2789FD7FEE80F1CF10F6551569A36FBDD08308234D3D1 |
| Malicious: | false |
| Reputation: | low |
| Preview: | L.....F.....R]...3...R]...3.....0.....P.O..i.....+00.../C:\.....t1....QK.X..Users.`.....QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=...U.....A.l.b.u.s.....z.1.....hT....Desktop.d....QK.XhT..*..._=.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,-.2.1.7.6.9.....h.2..0...TFz .WF0SLQ~1.DOC..L.....hT..hT..*...r.....'.W.F.0.S.l.Q.W.K.r.1...d.o.c.x.....y.....8...[.....?J.....C:\Users\.#.....\745481\Users.user\Desktop\WF0SLQWkr1.docx.&.....\.....\.....\D.e.s.k.t.o.p.\W.F.0.S.l.Q.W.K.r.1...d.o.c.x.....;..LB.)...Ag.....1SPS.XF.L8C....&m.m.....~...S-.1.-5.-2.1.-9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-1.0.0.6.....`.....X.....745481.....D_....3N...W...9...N.....[D_....3N...W...9. |


| | |
|--|--|
| C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 72 |
| Entropy (8bit): | 4.64599757904104 |
| Encrypted: | false |
| SSDEEP: | 3:bDuMJlqY6edrSmxW5jV7edrSv:bCeNojVcl |
| MD5: | EEB53A21B4BCA30826B0839173E17316 |
| SHA1: | 9969EC418E38AA968D829DDAA057E4BAA4CBF6B5 |
| SHA-256: | 69EE2A62099FC9FE91C0E9327F68041CBBCC23D4C3A003D99B184A174B49BC96 |

| | |
|-------------|--|
| SHA-512: | EBA7AB080E155C2D162374F2BB001B184FBBFB55B2CB32932D461F52330BD7A969863226C67A4A252A6873C21E4A6A5408D3F779BA2AD925F7DD2F6CD3B6F5C5 |
| Malicious: | false |
| Reputation: | low |
| Preview: | [folders]..Templates.LNK=0..WF0SIQWKr1.LNK=0..[misc]..WF0SIQWKr1.LNK=0.. |


| | |
|---|--|
| C:\Users\user\AppData\Roaming\Microsoft\Templates\~\$Normal.dotm | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.503835550707525 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/I |
| MD5: | C5E24006AFAC8C2659023AD09A07EB0F |
| SHA1: | 4B7B834BEDADF0A2764743E021D40C55A51F284 |
| SHA-256: | 7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E |
| SHA-512: | 673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | .user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x... |

| | |
|---|--|
| C:\Users\user\Desktop\~\$0SIQWKr1.docx | |
| Process: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 162 |
| Entropy (8bit): | 2.503835550707525 |
| Encrypted: | false |
| SSDEEP: | 3:vrJlaCkWtVyEJbiJk/p2TKWWhMGHiV/ln:vdsCkWttViJkh2TKHM9V/I |
| MD5: | C5E24006AFAC8C2659023AD09A07EB0F |
| SHA1: | 4B7B834BEDADF0A2764743E021D40C55A51F284 |
| SHA-256: | 7C9E6D71E3F53D37A78CCE23FA21D259365A9571C6C3A01E8D216586177BA87E |
| SHA-512: | 673649AF8318514414758F92756D408FB6F0CA4859CB2994A921E288126561A7B4EB3C7D824CC90352D939952EA167A473A4282838362B36E85B701A4B582396 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | .user.....A.l.b.u.s.....p.....16.....26.....@36.....36.....z.....p46.....x... |


| | |
|-------------------------|---|
| Static File Info | |
| General | |
| File type: | Microsoft OOXML |
| Entropy (8bit): | 7.762329445476857 |
| TrID: | <ul style="list-style-type: none">Word Microsoft Office Open XML Format document (49504/1) 49.01%Word Microsoft Office Open XML Format document (43504/1) 43.07%ZIP compressed archive (8000/1) 7.92% |
| File name: | WF0SIQWKr1.docx |
| File size: | 12519 |
| MD5: | 783f850d06c9f1286eb9b1bda0af0bce |
| SHA1: | 08011884c9bed126b4cfbadad4a4be5063805230 |
| SHA256: | 211a1f74eea68ebe7178d90f0df0446a87cdda865145c397b7a32e253086139e |
| SHA512: | fcab796a185f90db166c6fc335dd54db3b51856b3daa46905dfa5641ced9140ae18cf601e7b93a511c2d77b94e21bdddc7b2e23a49d358fb3960be781070a6f |
| SSDEEP: | 384:Fkv41E49wKxhpp+gX6eILi7RMobB/P/sQGwZRB98PG0S:evyE4aWfKetIV9PDxgA |
| TLSH: | 1D428D33C7074835D0ABBA870D95483EA75CD45E9D2A09F3A94E2D04CE26EB1B0778D |
| File Content Preview: | PK.....!.....!R.....[Content_Types].xml...N.1...M .Mo.[.....?.J">@ig..6.....e.....l.9. .d:..+..!.....'2.:..g.x.<voD...Q.x{..P.....&.f..X.9Q.....*.y...R.T).c.....S.j.1..C.....5.nH.8..].Xg.B...V.u...KJw...r..S....B.L.+...t 5....*. |

| | |
|---|------------------|
| File Icon | |
|  | |
| Icon Hash: | e4e6a2a2a4b4b4a4 |

Network Behavior

| |
|---|
|  No network behavior found |
|---|

Statistics

| |
|---|
|  No statistics |
|---|

System Behavior

Analysis Process: WINWORD.EXE PID: 1008, Parent PID: 576

General

| | |
|-------------------------------|---|
| Target ID: | 0 |
| Start time: | 08:18:11 |
| Start date: | 20/06/2022 |
| Path: | C:\Program Files\Microsoft Office\Office14\WINWORD.EXE |
| Wow64 process (32bit): | false |
| Commandline: | "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding |
| Imagebase: | 0x13f9c0000 |
| File size: | 1423704 bytes |
| MD5 hash: | 9EE74859D22DAE61F1750B3A1BACB6F5 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | high |

File Activities

| File Created | | | | | | | |
|-------------------------------------|---|------------|--|-----------------|-------|----------------|------------------|
| File Path | Access | Attributes | Options | Completion | Count | Source Address | Symbol |
| C:\Users\user\AppData\Local\Temp\VE | read data or list directory synchronize | device | directory file synchronous io non alert open for backup ident open reparse point | success or wait | 1 | 6E1A2B14 | CreateDirectoryA |

| File Deleted | | | | |
|--|-----------------|-------|----------------|---------|
| File Path | Completion | Count | Source Address | Symbol |
| C:\Users\user\Desktop\-\$0SIQWkr1.docx | success or wait | 1 | 6E220648 | unknown |

| Old File Path | New File Path | | | Completion | Count | Source Address | Symbol |
|---------------|---------------|--|--|------------|-------|----------------|--------|
|---------------|---------------|--|--|------------|-------|----------------|--------|

| File Path | Offset | Length | Value | Ascii | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|-------|-------|------------|-------|----------------|--------|
|-----------|--------|--------|-------|-------|------------|-------|----------------|--------|

| File Read | | | | | | | | |
|-----------|--|--|--|--|--|--|--|--|
|-----------|--|--|--|--|--|--|--|--|

| Key Path | Name | Type | Old Data | New Data | Completion | Count | Source Address | Symbol |
|----------|------|------|----------|---|------------|-------|----------------|--------|
| | | | | 00 FF FF FF | | | | |
| | | | | FF | | | | |

FF

Disassembly

 No disassembly