

SnipBook V73 – Dateioperationen des Word-Makros

Was das Makro **Word2HTMLSnipBook** im Hintergrund tut – und warum Antivirusprogramme manchmal reagieren

BETEILIGTE ORDNER & DATEIEN

-  **Word-SnipBook-Viewer** ← Ordner neben der DOTM
 -  Word-SnipBook-v73.dotm ← Makro-Vorlage (Startpunkt)
 -  **SnipBook-Tools**
 -  SnipBook-Viewer-Template-V73.html ← Viewer-Template (Quelle)
 -  MeinDokument.htm ← Ausgabe (wird erzeugt / überschrieben)
 -  MeinDokument_files\ ← Bilder der Ausgabe
-  %TEMP%\SnipBookWork\MeinDokument-20260405-143022\ ← temporärer Arbeitsordner
 -  MeinDokument-SnipBook-TMP-EXPORT.docx ← temporäre DOCX-Kopie
 -  MeinDokument.htm ← Word-Roh-HTML (temporär)
 -  MeinDokument_files\ ← Bilder aus Word-Export (temporär)
 -  snipbook_out_tmp.htm ← Schreib-Puffer vor Kopie ans Ziel

DOTM / Viewer (Quellen, nur gelesen)

Temp-Ordner (größtenteils zurückbleibend, nur .htm wird gelöscht)

Ausgabe (neben der DOTM)

ABLAUF SCHRITT FÜR SCHRITT

1

Viewer-Template suchen & lesen

LESEN Das Makro sucht SnipBook-Viewer-Template-V73.html im eigenen Ordner bzw. im Unterordner SnipBook-Tools\ und liest die Datei als UTF-8-Text ein (via ADODB.Stream).

2

Temporäre DOCX-Kopie erzeugen

SCHREIBEN Das aktive Dokument wird als Kopie in den Temp-Ordner gespeichert – damit das Original nicht verändert wird.

```
%TEMP%\SnipBookWork\MeinDokument-[timestamp]\MeinDokument-SnipBook-TMP-EXPORT.docx
```

3

Word-Export: Gefiltertes HTML

SCHREIBEN Word öffnet die Temp-DOCX und speichert sie als *Gefilterte Webseite*. Dabei entstehen automatisch eine .htm-Datei und ein _files\-Ordner mit allen Bildern – beides im Temp-Ordner.

```
%TEMP%\SnipBookWork\...\MeinDokument.htm + _files\
```

4

Word-HTML einlesen & Viewer injizieren

LESEN Das Temp-HTML wird gelesen (via ADODB.Stream). Dann werden CSS, UI-HTML und JavaScript aus dem Viewer-Template in das Word-HTML eingefügt – alles im Arbeitsspeicher, keine Datei-Schreiboperation.

5

Video- & GIF-Platzhalter patchen

LESEN Bilder mit dem Alt-Text `[[GIF|...]]` oder `[[VIDEO:...|...]]` werden erkannt. GIF-Dateien werden binär gelesen und als Base64-String direkt in das HTML eingebettet (kein externer Zugriff zur Laufzeit nötig).

6

Bilderordner ans Ziel kopieren

KOPIEREN Der Temp-_files\ -Ordner wird in den Zielordner neben der DOTM kopiert (via FSO.CopyFolder).

```
%TEMP%\...\MeinDokument_files\ → Word-SnipBook-Viewer\MeinDokument_files\
```

7

Fertige HTM ans Ziel schreiben

SCHREIBEN Das fertige HTML wird zunächst als Puffer-Datei in %TEMP% gespeichert, dann per FSO.CopyFile in den Zielordner kopiert. Dieser zweistufige Weg reduziert die Wahrscheinlichkeit, dass Antivirusprogramme den Schreibvorgang blockieren.

```
%TEMP%\snipbook_out_tmp.htm → Word-SnipBook-Viewer\MeinDokument.htm
```

8

Aufräumen & Browser öffnen

LÖSCHEN Nur die temporäre .htm-Datei im Temp-Ordner wird gelöscht. Die temporäre DOCX-Kopie, der _files\ -Ordner und der timestamped Unterordner bleiben in %TEMP%\SnipBookWork\ zurück – bei jedem Durchlauf kommt ein neuer Ordner hinzu. Windows räumt %TEMP% gelegentlich selbst auf. Die fertige HTM-Datei wird über Word's FollowHyperlink im Standardbrowser geöffnet – ohne den Umweg über cmd.exe.

WARUM ANTIVIRUSPROGRAMME REAGIEREN KÖNNEN



WINWORD.EXE startet cmd.exe



ADODB.Stream liest & schreibt Dateien

Frühere Versionen öffneten den Browser über Shell "cmd /c start ...". Die Kette WINWORD → cmd.exe ist ein klassisches Malware-Muster und wurde von Bitdefender als *SuspiciousBehavior* blockiert.

V73: ersetzt durch FollowHyperlink.

Für UTF-8-korrektes Lesen und Schreiben wird ADODB.Stream verwendet – ein COM-Objekt, das auch von Malware genutzt wird. Manche AV-Programme quarantinierten es vorsorglich.

V73: Pure-VBA-Fallback wenn ADODB fehlt.



Binärdateien lesen + Base64-Encoding

Das GIF-Embedding liest Bilddateien binär und kodiert sie als Base64-String. Dieses Muster ähnelt dem Auslesen und Verpacken von Daten – ein Verhalten, das AV-Heuristiken als potenzielle Exfiltration einstufen können.



Schreiben in OneDrive-Ordner

Wenn WINWORD.EXE in einen OneDrive-synchronisierten Ordner schreibt, sieht das für Verhaltenserkennungen wie „Office-Makro lädt Daten in die Cloud hoch“ aus – auch wenn es nur die eigene HTM-Ausgabe ist.



Kein Netzwerkzugriff

Das Makro greift zu keinem Zeitpunkt auf das Internet zu. Alle Ressourcen (jQuery, Slick, Fonts) werden lokal aus dem SnipBook-Tools\ -Ordner geladen.



Kein Systemordner-Zugriff

Alle Schreiboperationen beschränken sich auf den eigenen Arbeitsordner und %TEMP%\SnipBookWork\ . System- und Registry-Zugriffe finden nicht statt.

LÖSUNG BEI ANHALTENDER BLOCKIERUNG



Bitdefender – Erweiterte Bedrohungsabwehr: Ausnahme eintragen

Bitdefender → Schutz → Erweiterte Bedrohungsabwehr → Ausnahmen → Anwendung hinzufügen

Dort WINWORD.EXE eintragen. Diese Einstellung gilt nur für die Verhaltensüberwachung – der normale Virenschutz bleibt aktiv.

Alternativ: Den Ausgabeordner als Ausnahme im Echtzeit-Virenschutz eintragen, damit der Schreibzugriff nicht blockiert wird.