

Ransomware: „DataENcryption made easy“

Camp++ 0x7e1

The Word

- “Ransom” = Ransom
- Blackmailing

History

1989

AIDS TROJAN DISK

distributed/infected via floppy disk

developer was caught and put into jail

first internet attack

“TROJ_PGPCODER.A”

couple of hundred \$ ransom

Today

A lot of infections

In the meantime (big) companies affected

1/4 of the people pay the ransom
(estimated number of unknown
cases higher)^[0]

Different versions of Ransomware

A Selection

- Locky
- TeslaCrypt
- CryptoWall 4.0
- Petya
- Cerber
- CTB-Locker

Rot: No Decrypter available
Grün: Decrypter available

Ransomware in reality

Ransomware: US-Krankenhaus zahlt 40 Bitcoins Lösegeld

heise online 18.02.2016 10:34 Uhr - Axel Kannenberg

vorlesen



Bitcoins im Wert von 15.000 Euro blätterte ein Krankenhaus in Los Angeles hin, um seine von einem Erpressungstrojaner verschlüsselten Daten wieder freizukriegen. Das sei der schnellste Weg gewesen, sagte der Krankenhaus-Chef.

Ähnliche Artikel

TeslaCrypt 2.0 entschlüsselt

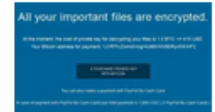
Die Ransomware TeslaCrypt ist geknackt und betroffene Nutzer können auch ohne das Zahlen von Lösegeld wieder Zugriff auf ihre verschlüsselten Daten...



heise Security 17

nachgehakt: Was können Opfer von Erpressungstrojanern tun?

Momentan grassiert eine neue Version des Erpressungstrojaners TeslaCrypt, der Dateien und Bilder auf den Festplatten verschlüsselt und nur gegen...



ct 31

<http://www.heise.de/newsticker/meldung/Ransomware-US-Krankenhaus-zahlt-40-Bitcoins-Loesegeld-3109956.html>

current Ransomware: Popcorn Time

POPCORN TIME

Ransomware gibt Daten frei, wenn man Freunde infiziert

12.12.16, 11:56 [✉ Mail an die Redaktion](#)




Foto: MalwareHunterTeam

FEATURED



FUTURELAB261
"Keine weiteren Invest
ORF-Start-up-Cluster v

current Ransomware: Goldeneye

 **golem.de**
IT-NEWS FÜR PROFIS

HOME TICKER VIDEO

TOP-THEMEN: [Telekom](#) [Apple](#) [Amazon](#) [Auto](#) [Golem retro_](#) [Microsoft](#) [mehr...](#)

SUCHEN

SERVICES: [PREISVERGLEICH](#) [STELLENMARKT](#) [TOP-ANGEBOTE](#) [IT-KÖPFE](#) **NEU** [ABO](#)

PETYA-VARIANTE

Goldeneye-Ransomware verschickt überzeugende Bewerbungen

Kurz vor dem Jahresende gibt es erneut eine größere [Ransomware-Kampagne](#) in Deutschland. Kriminelle verschicken mit Goldeneye professionell aussehende Bewerbungen an Personalabteilungen - und nutzen möglicherweise Informationen des Arbeitsamtes.

Der Verschlüsselungstrojaner Goldeneye verbreitet sich zurzeit offenbar mit großer Geschwindigkeit in Deutschland. Es handelt sich nicht um eine grundlegende Neuentwicklung, sondern um eine Variante der bekannten Petya-Malware. Der Titel ist offenbar eine Anlehnung an einen James-Bond-Film, wie [Bleepingcomputers berichtet](#).



Pierce Brosnan als James Bond in Golden Eye (Bild: Getty Images)

Datum: 7.12.2016, 17:04

Autor: [Hauke Gierow](#)

Themen: [Ransomware](#), [Anti-Virus](#), [Bitcoin](#), [James Bond](#), [Malware](#), [Trojaner](#), [Virens scanner](#), [Applikationen](#), [Security](#)

Teilen:



A guide to getting infected



Example email, with links to Ransomware

Bewerbung von Wolf

Sehr geehrte Damen und Herren,

da ich auf der Suche nach einer neuen beruflichen Herausforderung bin, möchte ich mich hiermit bei Ihnen bewerben. Da ich bereits mehrere Jahre in diesem Bereich gearbeitet habe und zurzeit Arbeit suchend bin, möchte ich mich bei Ihnen bewerben.

Nach meiner Fachhochschulreife und meinen bisherigen Praktika konnte ich bereits Erfahrungen in unterschiedlichen Bereichen sammeln.

Sie finden in mir einen belastbaren, einsatzbereiten, flexiblen, selbstständigen und zuverlässigen Mitarbeiter mit hoher Teamorientierung. Das Einarbeiten in neue Aufgabengebiete bereitet mir keine Probleme.

Ich würde mich sehr freuen, wenn meine Bewerbung Ihr Interesse wecken konnte und ich mich persönlich bei Ihnen vorstellen darf. Über ein persönliches Gespräch freue ich mich sehr.

Mit freundlichem Gruß

Dirk Wolf

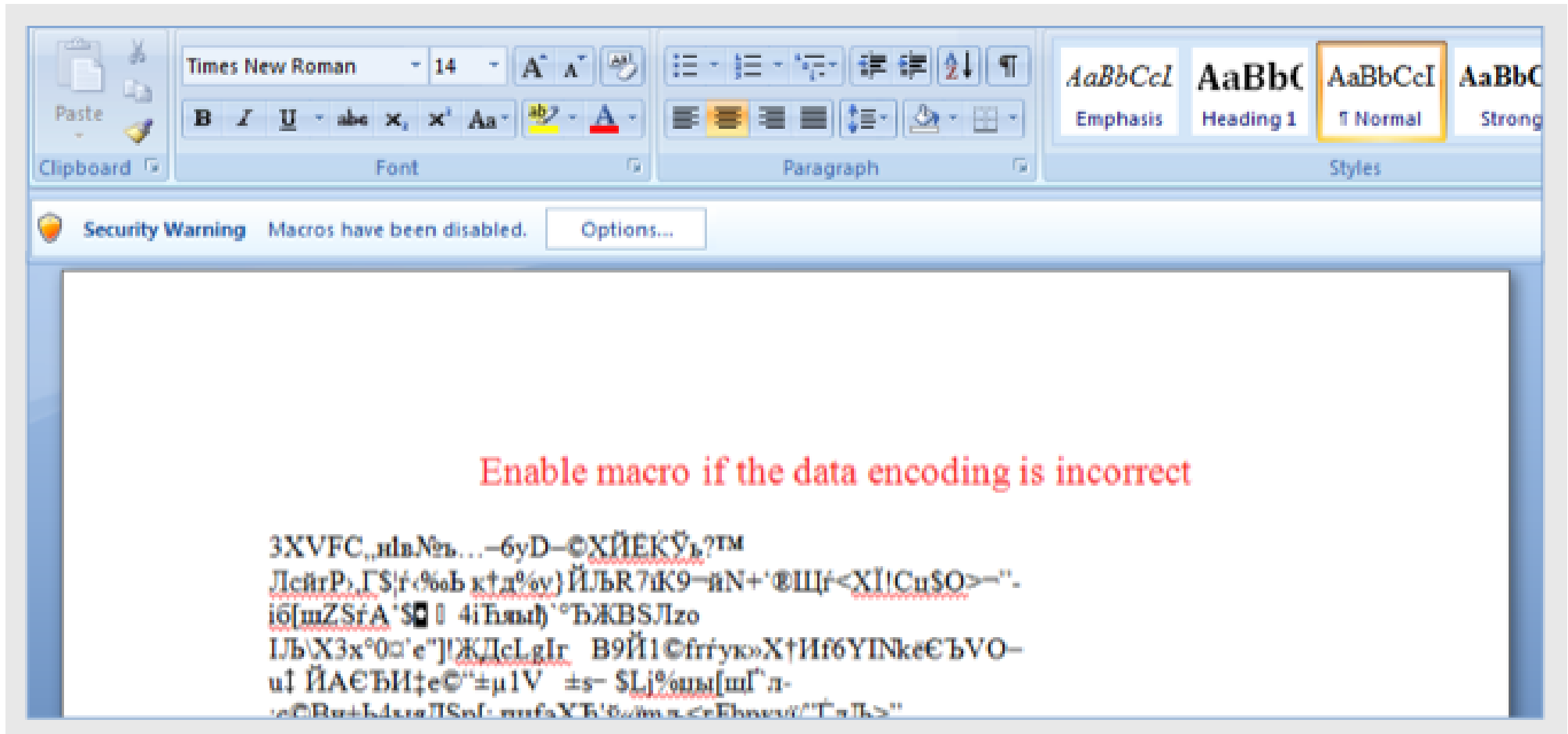
Anhänge
Lebenslauf und Arbeitszeugnis

<https://www.dropbox.com/sh/o6qalep9dfohcpl/AADBwM0UbHi341tXo9m3tXwka?dl=0>

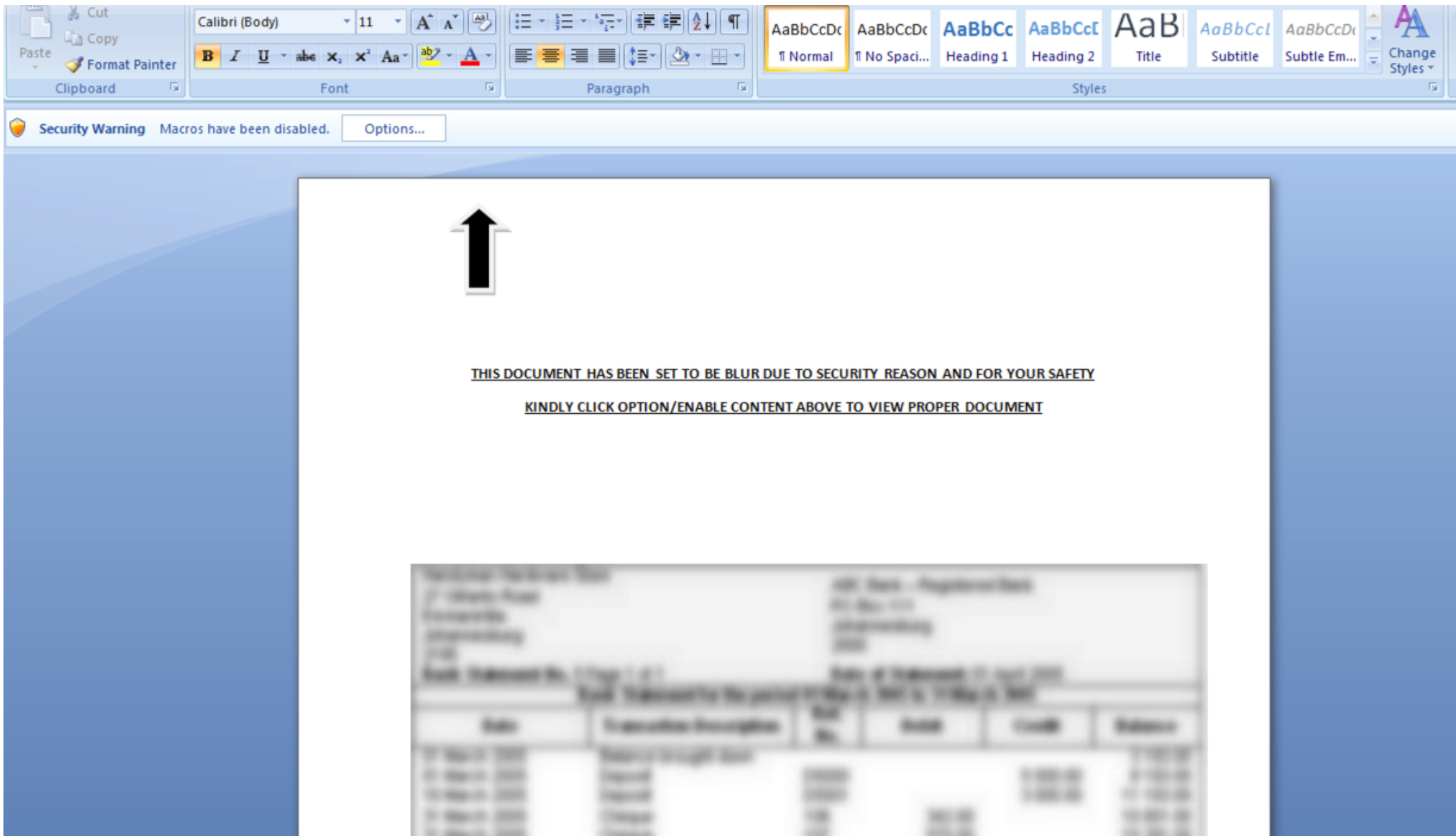
Die vollständige Bewerbungsmappe habe ich meine Dropbox geladen, weil die Datei für die Email zu groß war - Entschuldigen Sie bitte!

Office (Word) Macro

Example of Word-Macro Malware



Example of Word-Macro Malware



PDF

Through security holes in PDF format.
often exploited using unknown “zero-day”

Adobe Flash (Player)

(Java) Drive by Attack

What happens exactly?

- Different methods
- Different data extensions encrypted
- Blackmailing message
- Optional: Countdown
- Deletion of data
- Possible: blackmail with data

How it is encrypted?

- Files → symmetric with AES
- AES Key → RSA Public Key
- On Server → RSA Private Key

Other way of encryption also possible!

Petya/Goldeneye → File System Table & MBR

How to protect?

Backups

**YOU SAY YOU DON'T
USE BACKUPS?**

**TELL ME MORE ABOUT THIS
GENIUS PLAN FOR DATA LOSS**

Various ways of Backups

- Single Files
- Image
- incremental
- Remote Backups on fileserver
- Differential

Think about

- Software Licenses
- Userprofile of programs
 - Firefox
 - Thunderbird
- passwords

Copies of the files on the local computer are not safe.

Also not on a another partition of the same HDD!

BACKUP ALL THE THINGS



Test your backup!

In worst case restoring the backup doesn't work
testing is essential!

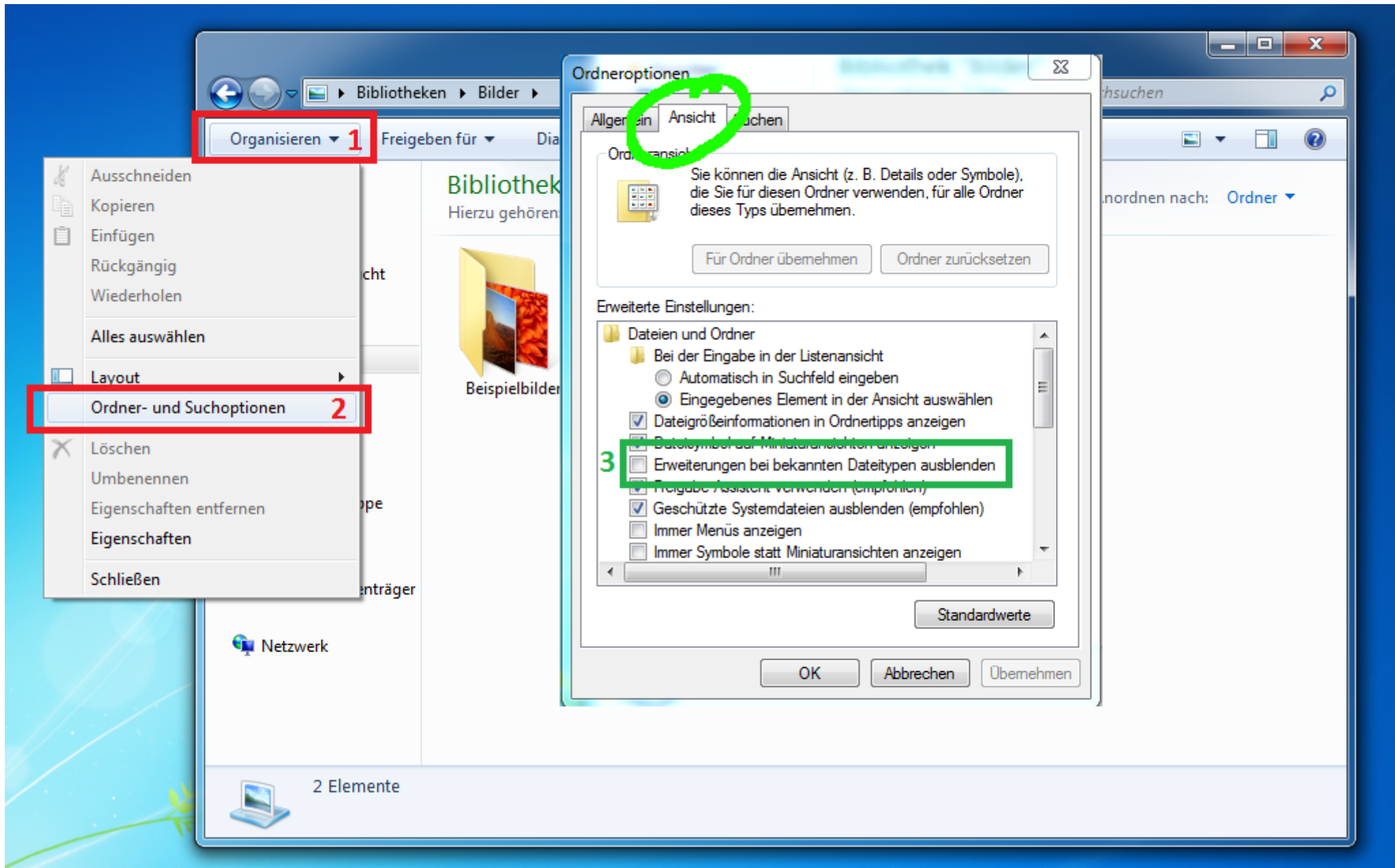
Software recommendation

- Paragon Backup & Recovery 14 Free
- Areca Backup
- AOMEI Backupper
- Windows internal Backup tool

Up-to-date anti virus (AV) software

Up-to-date Operating System + Browser
+ programs (Adobe PDF)

Turn on windows file extensions



Deactivate Adobe Flash
better: uninstall

Email + attachment mistrust

No administrator privileges!

Work with limited user privileges

Doesn't protect from Ransomware!
Data will still be encrypted

provides false security

no plugging in of (Un)known Flash drives

You can check suspicious files online

<https://www.virustotal.com>

Don't upload private data!

Use Linux!

Userfriendly Systems:

- Ubuntu
- Linux Mint

BRAIN.EXE



USE YOU MUST

Backup?

Backup

BACKUP!

Summary

infected, what to do?

- 1) Turn off computer immediately
- 2) Boot live System (from flash drive/CD/DVD)
- 3) Detect Ransomware type
- 4) Rescue data
- 5) Reinstall OS
- 6) Restore Backup

HAVE YOU



NO BACKUP?!

IT'S DEMO TIME!

WHAT COULD POSSIBLY GO WRONG?

Questions?

Further Sources & Informationen

<https://ransomware.at/>

Creator

CC-BY:

Hetti - <https://twitter.com/Th3PeKo>