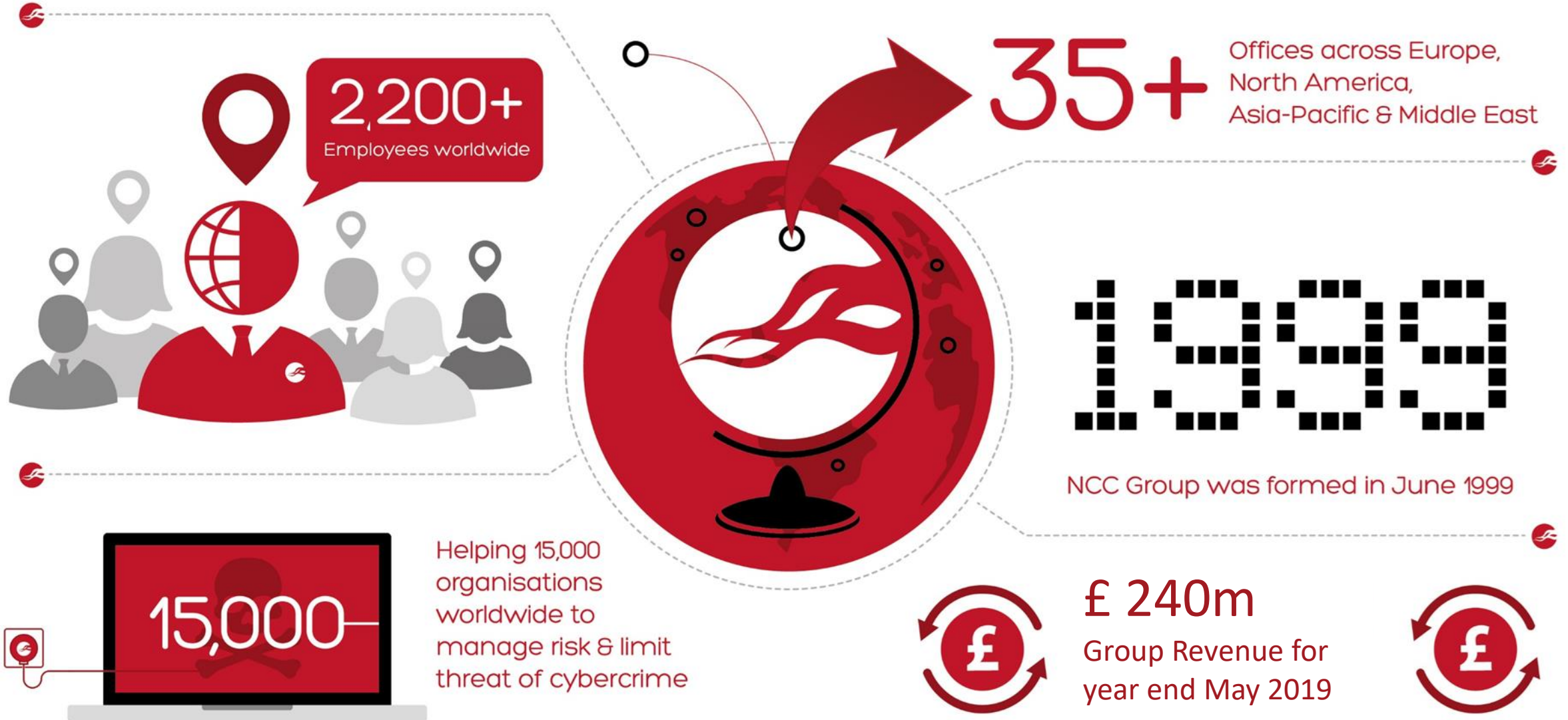




**FOX IT**  
part of nccgroup

Tim auf der Landwehr

Senior Security Expert







































# TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles



NAC  
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]











Abfahrt

Linie

Ziel

Gleis

Zeit

Über

Nach

Olbernhau

Hbf

(S) Hbf

g-B. Süd

Hbf

Aue (Sachs)

Dresden Hbf

22:10  
RB81

22:30  
RB30

22:31  
RB30

22:36  
RB80

22:36  
RB45

22:44  
RE6

22:45  
RB89

22:50

Flöha - Pockau-Lengefeld

Flöha - Freiberg  
- Fährt heute

Hohenstein

Flöha - Zsch

irt heute von  
Geithain - B

Einsiedel - Thalheim (Erzgeb)

Flöha - Freiberg (Sachs) - Tharandt

Oops, your files have been encrypted!

Was geschah mit meinem Computer?  
Ihre wichtigen Dateien sind verschlüsselt. Ihre wichtigen Dokumente, Fotos, Videos, Datenbankdateien und noch viele andere Dateien sind verschlüsselt. Sie sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.

Kann ich meine Dateien wiederherstellen?  
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber Sie haben nicht genug Zeit. Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf "Decrypt" klicken. Aber wenn Sie alle Ihre Dateien entschlüsseln wollen, müssen Sie bezahlen. Sie haben nur 3 Tage, um die Zahlung anzufordern. Danach wird der Preis verdoppelt. Auch wenn Sie nicht in 7 Tagen bezahlt haben, können Sie Ihre Dateien nicht für immer wiederherstellen. Wir haben keine Voraussetzungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.

Wie bezahle ich?  
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf "About bitcoin".

Send \$300 worth of bitcoin to this address:  
129YDPgusZ9NyMgw519p7AABjrdSMw

Check Payment Decrypt

Payment will be raised on  
5/15/2017 22:50:58  
Time Left  
02:23:18:55

Your files will be lost on  
5/15/2017 22:50:58  
Time Left  
06:23:18:55

About bitcoin  
How to buy bitcoin?  
Contact Us









# COLONIAL PIPELINE



## PELHAM JUNCTION AND TANK FARM

EMERGENCY NO. CALL TOLL FREE: 1-800-926-2728

### WARNING: NO TRESPASSING

RESTRICTED, OFFENSE TO OFFENSE DAMAGE, OR EXCESSIVE DAMAGE UP TO \$500 FINE + 1 YEAR IMPRISONMENT

#### NOTICE

ALL VEHICLES AND  
PERSONNEL ENTERING  
OR LEAVING THE PREMISES  
SUBJECT TO SEARCH

#### DANGER

NO SMOKING  
NO FLAMES  
NO SPARKS



#### NOTICE

MINIMUM 8 CAL.  
AR/FR  
PPE  
BEYOND THIS POINT



#### NOTICE



SAFETY GLASSES,  
SAFETY SHOES &  
HARD HATS ARE  
REQUIRED BEYOND  
THIS POINT

SPEED  
LIMIT  
**10**



#### WARNING

Recorded  
VIDEO SURVEILLANCE  
Grabación de VIDEO vigilancia

Electronic equipment  
is used to monitor the  
premises of any person  
controlled against this  
facility.

Equipos electrónicos  
se usan para monitorear el  
establecimiento de las instalaciones  
controladas contra de esta  
instalación.

**WARNING**  
ABOVE GROUND  
PIPING

ALL VISITORS OR  
CONTRACTORS MUST  
SIGN IN AT BLDG

**NOTICE**  
AUTHORIZED  
PERSONNEL  
ONLY



Can You *find* the  
the MISTAKE

1 2 3 4 5 6 7 8 9



[www.sdv.de](http://www.sdv.de)

[www.sdv-ag.de](http://www.sdv-ag.de)

[www.sdv.ag](http://www.sdv.ag)

[sdv.ag.de](http://sdv.ag.de)



# Win.

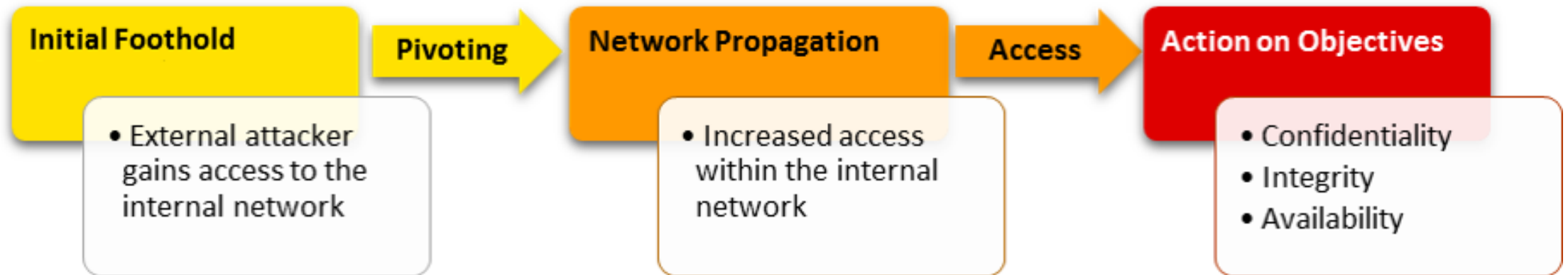
Chance to win an **iPhone X**\*

.....Click [here](#)!





# The unified Kill Chain









# Update!



Redmond, WA  
January 21, 2015









# Starke Passwörter





# Einzigartige Passwörter

[Home](#)[Notify me](#)[Domain search](#)[Who's been pwned](#)[Passwords](#)[API](#)[About](#)[Donate !\[\]\(faf942dc3e59ce8eb64b4ac481eca7e0\_img.jpg\) !\[\]\(f6b0299e0b5e4340e509b71914970da0\_img.jpg\)](#)

## ';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?

241

pwned websites

4,779,745,355

pwned accounts

56,046

pastes

53,242,773

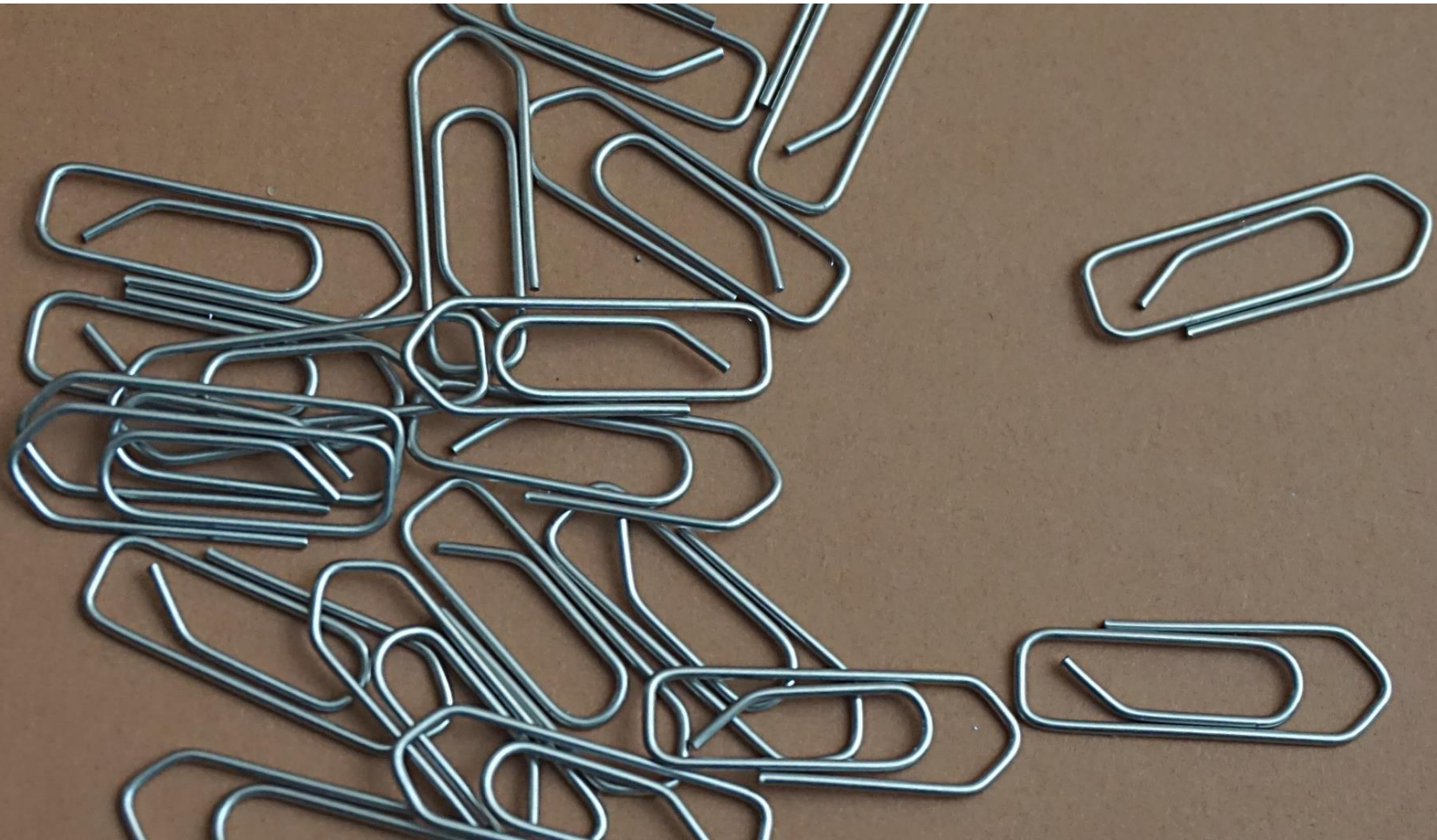
paste accounts



# Multi Factor Authentication



# Email Anhänge





BESTAND START INVOEGEN ONTWERPEN PAGINA-INDELING VERWIJZINGEN VERZENDLISTEN CONTROLLEREN BEELD

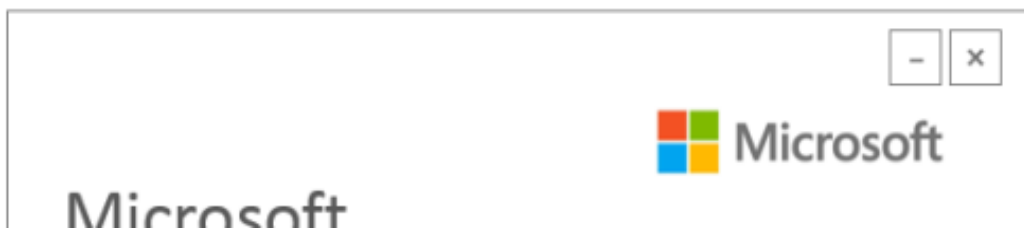
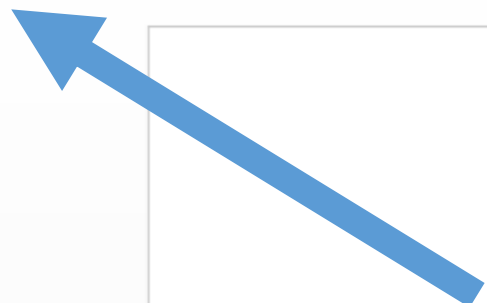
Plakken Knippen Kopieëren Opmaak kopiëren/plakken Klembord

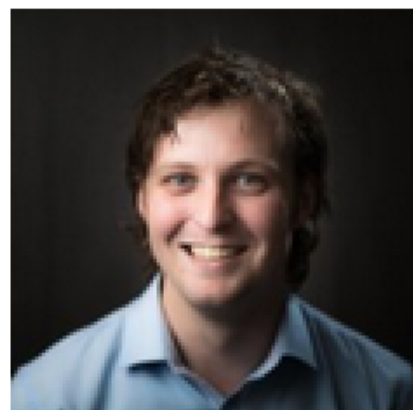
Lettertype Calibri 11 A A Aa B I U abc x<sub>2</sub> x<sup>2</sup> A ab A

Alinea

Stijlen AaBbCcDc AaBbCcDc AaBbC AaBbC AaBbC AaBbCcD AaBbCcDc AaBbCcDc AaBbCcDc AaBbCcDc AaBbCcDc 1 Standaard 1 Geen afs... Kop 1 Kop 2 Titel Ondertitel Subtiele b... Nadruk Intensieve...

! BEVEILIGINGSWAARSCHUWING Macro's zijn uitgeschakeld. Inhoud inschakelen





Hi Jennifer,

I'd like to connect with you on LinkedIn.

**Rutger Plak**

Forensic IT Expert at Fox-IT

Accept

View Profile

© 2015 LinkedIn Ireland Limited. LinkedIn, the LinkedIn logo, and InMail are registered trademarks of LinkedIn Corporation in the United States and/or other countries. All rights reserved.

<http://www.linkedin.com/pub/rutger-plak/>



# Öffentliches WLAN



# Gebrauchtgeräte





# Unbekannte USB sticks

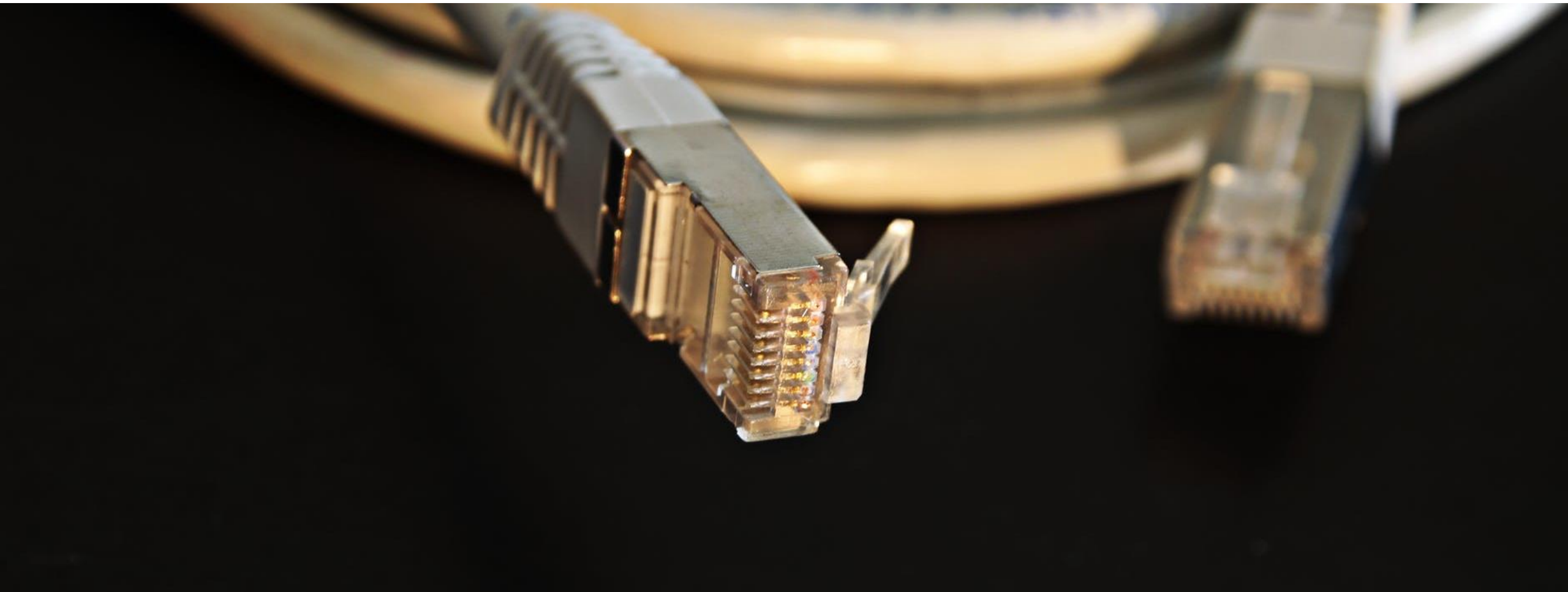


# Wie erkenne ich eine Malware Infektion?





# Netzwerkverbindung trennen



Zwischenfall melden





Fragen?

