Fishing for Phishers

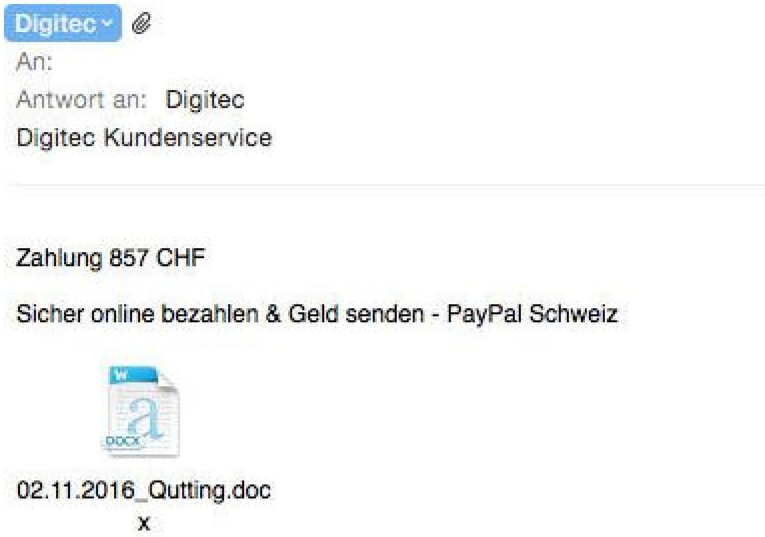
Who sends these emails anyway?

Who?

- Dominik Bärlocher
- Author
- Journalist
- Lifts weights
- dominik.baerlocher@digitec.ch

What?

- Fake mails
- Barely any text
- Attachment in .docx format



An:

Antwort an: Digitec

Digitec Kundenservice

Zahlung 857 CHF

Sicher online bezahlen & Geld senden - PayPal Schweiz

02.11.2016_Qutting.doc
x

1. OSINT

Open Source Intelligence: Using publicly available data in order to find or profile something or someone. (Basically stalking)

- **Google**
  Mighty search engine and big data monster that knows everything
- **Whois**
  Lots of people forget to activate privacy protection for their sites.
- **Bing**
  Looking for the same thing but with vastly different results.

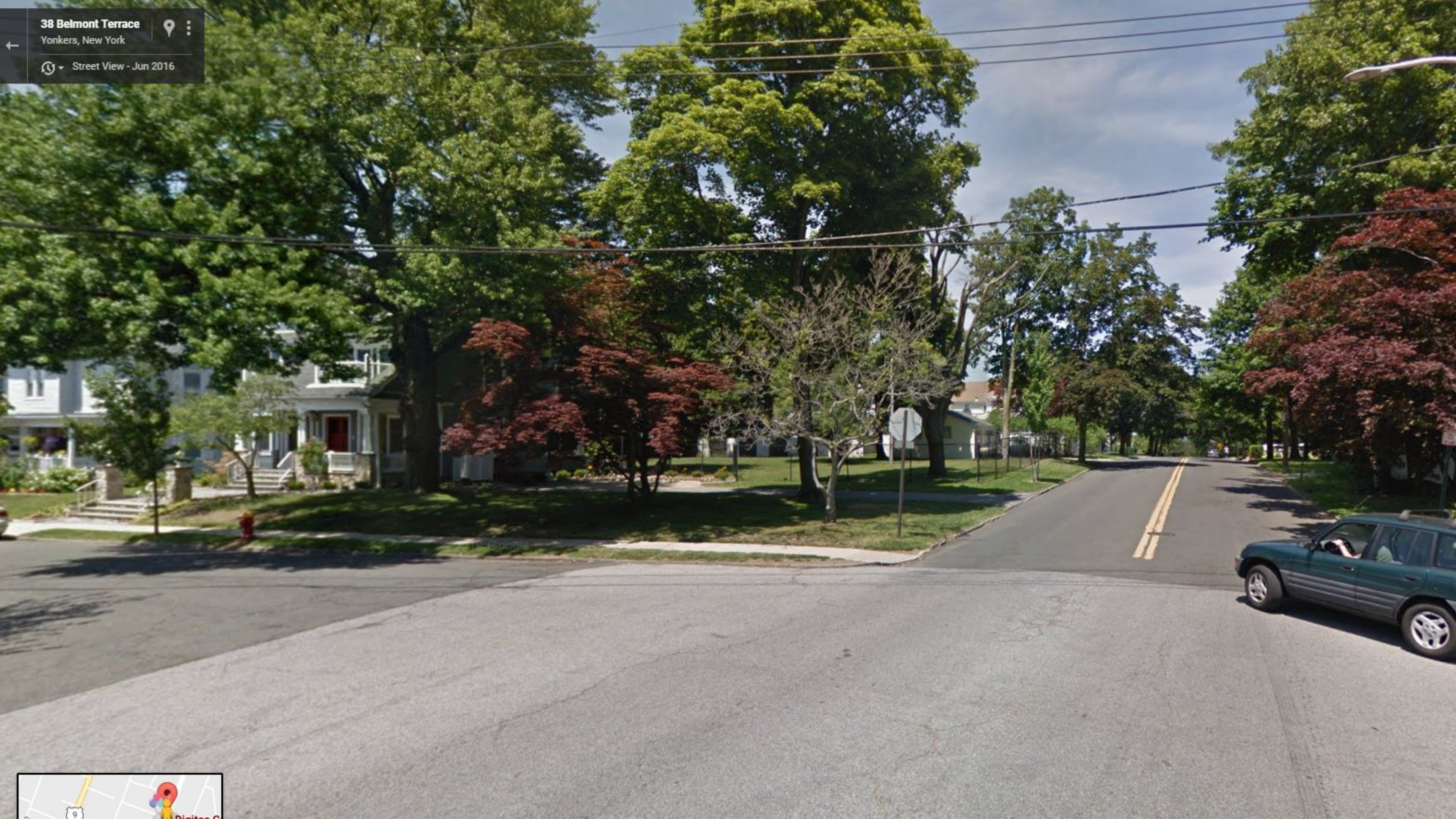
The Investigation Begins

- Mails sent from several addresses
- digitec@ropa-maschinenbau.de
- $something@digitec.com
- None of our domains
- Someone is spoofing mails from us

digitec.com

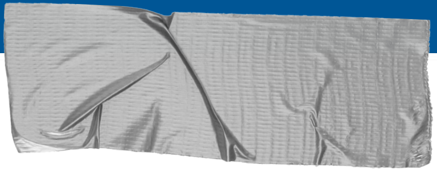
- Owner: Digitec Corporation
- Mail: digitec@compuserve.com
- Location: Yonkers, NY
- PO Box
- Google Maps has it listed
- What we're sure of: It's not us

Alpine
Mt Hope Cemetery
Saint Andrews
Palisades Interstate Pkwy
Hudson River
NEW YORK
Warburton Ave
High St
Ravensdale Rd
Jackson Ave
Tompkins Ave
HOMEFIELD
Nepperhan Ave
LEGOLAND® Discovery Center Westchester
Palisades Interstate Park
NORTHWEST YONKERS
Roberts Ave
Saw Mill River Pkwy
Sprain Rd
Curtis Ln
Palisade Ave
Park Ave
Morsemere Ave
Frederic St
Burhans Ave
Rossiter Ave
Buckingham Rd
Rockne Rd
Mile Square Rd
Tuckahoe Rd
Ridge Hill Boulevard
Bushey Ave
Lockwood Ave
Palmer Rd
Henry Hudson Dr
Ravine Ave
Orchard St
Ashburton Ave
Alexander St
N Broadway
Locust Hill Ave
Walnut St
Bennett Ave
Midland Ave
Yonkers Ave
Kingston Ave
Prescott St
Elm St
Oak St
Buena Vista Ave
Yonkers
Google


38 Belmont Terrace
Yonkers, New York
Street View - Jun 2016
9
Digitas C

Trail lost!

(But we’re not done!)



2. The Payload

The attachment: An analysis of what our informant sent us.

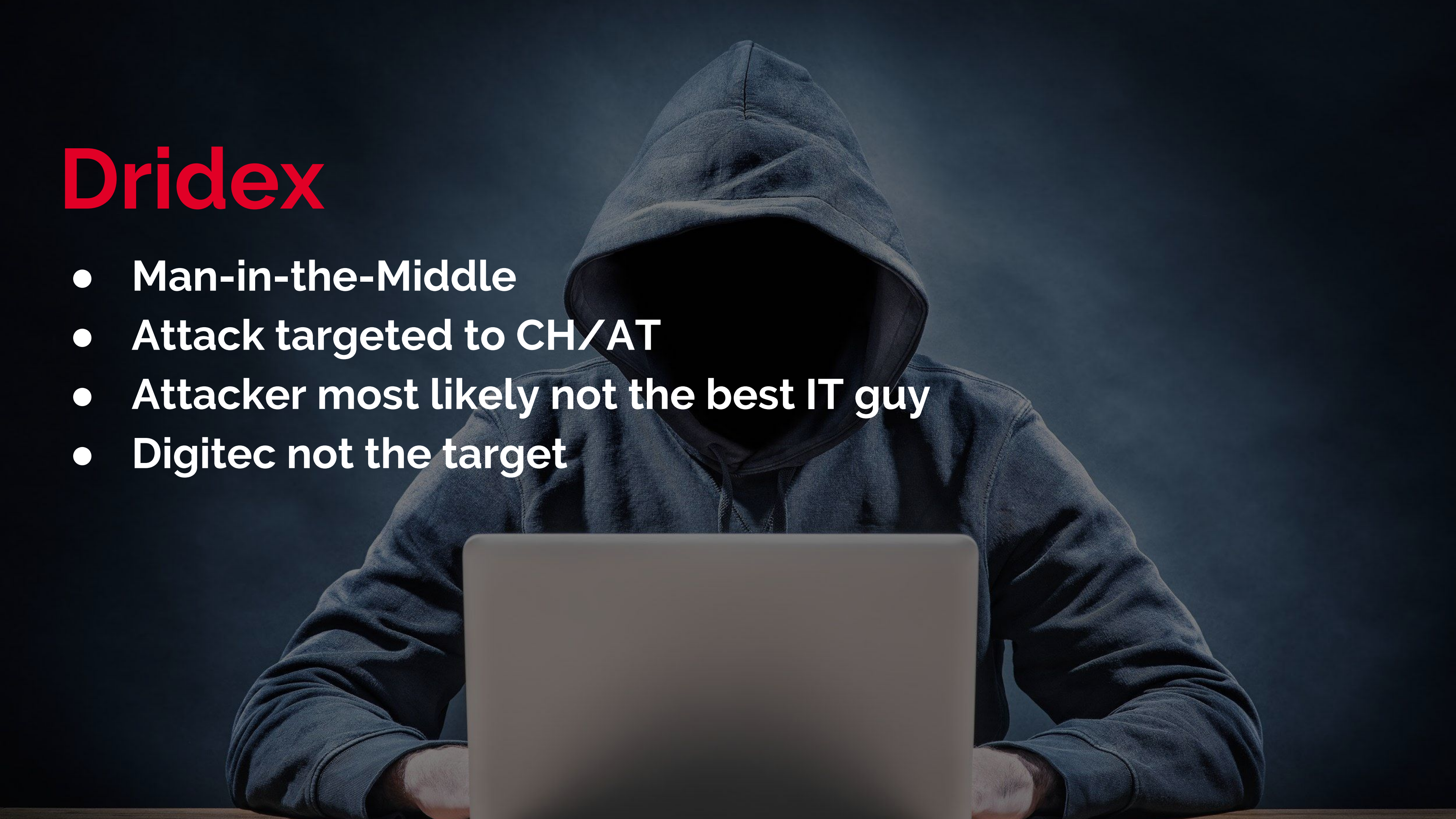
➔ **Reverse Engineering**
See if code can be decoded to read original code.

➔ **Untangle code**
What does it actually do? How can we reverse it?

➔ **Solution**
How do we keep our clients safe? Can they fix this themselves?

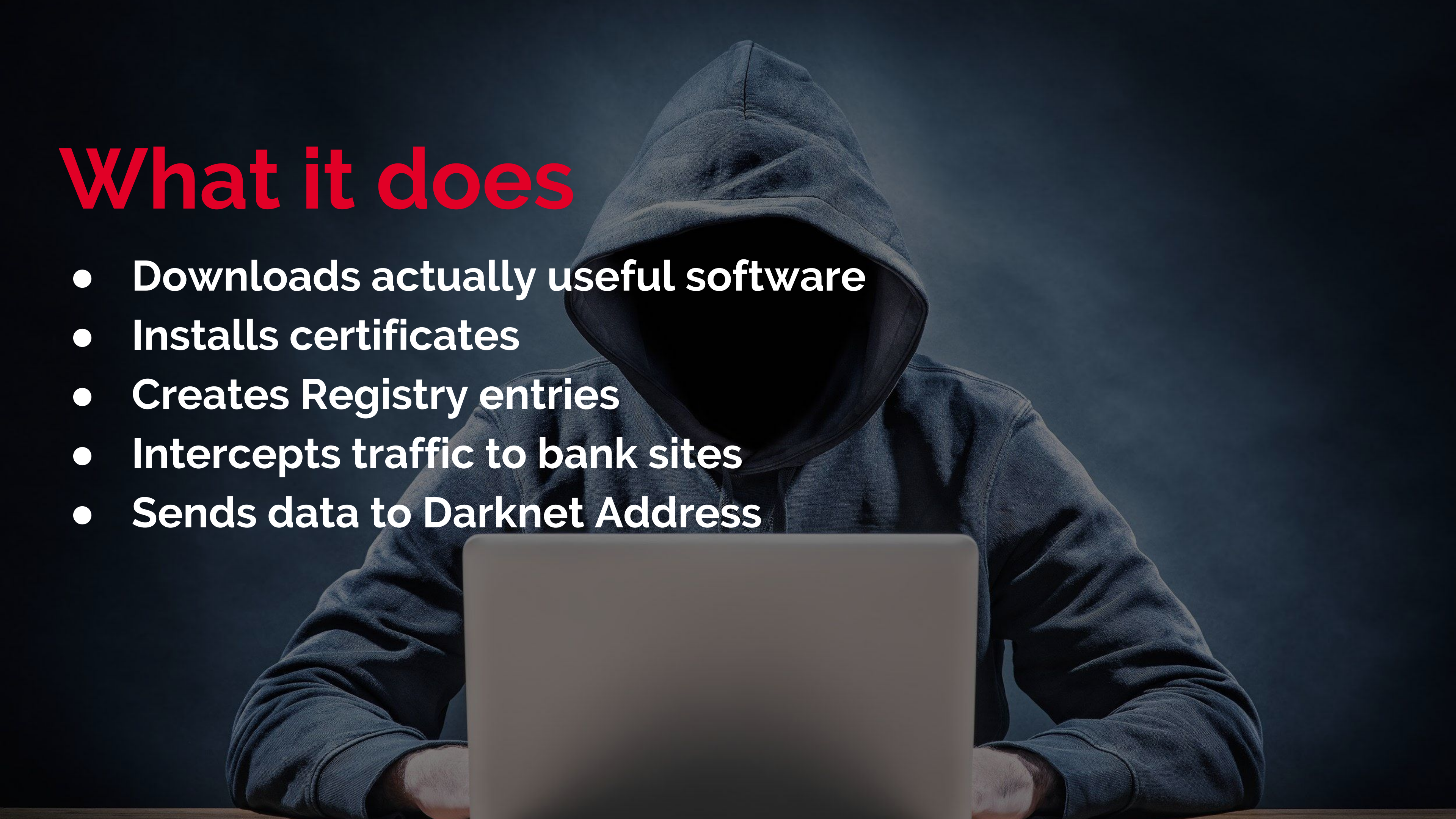
Dridex

- Man-in-the-Middle
- Attack targeted to CH/AT
- Attacker most likely not the best IT guy
- Digitec not the target



What it does

- Downloads actually useful software
- Installs certificates
- Creates Registry entries
- Intercepts traffic to bank sites
- Sends data to Darknet Address



3. The Impact

Going public: What to tell people and how to keep them safe..

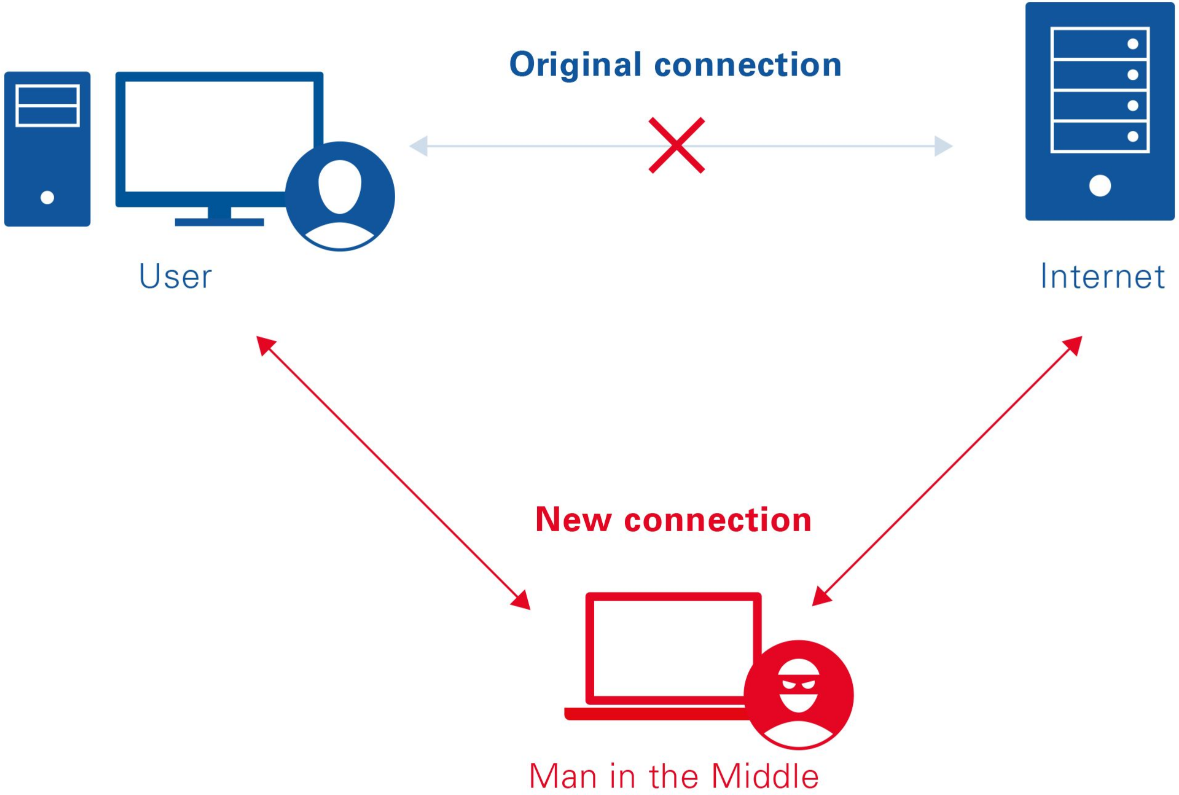
- ➔ **Journalistic Impact**
  Are our readers even interested in an article like this?
- ➔ **Awareness**
  What does it actually do? How can we reverse it?
- ➔ **Solution**
  How do we keep our clients safe? Can they fix this themselves?

The Aftermath

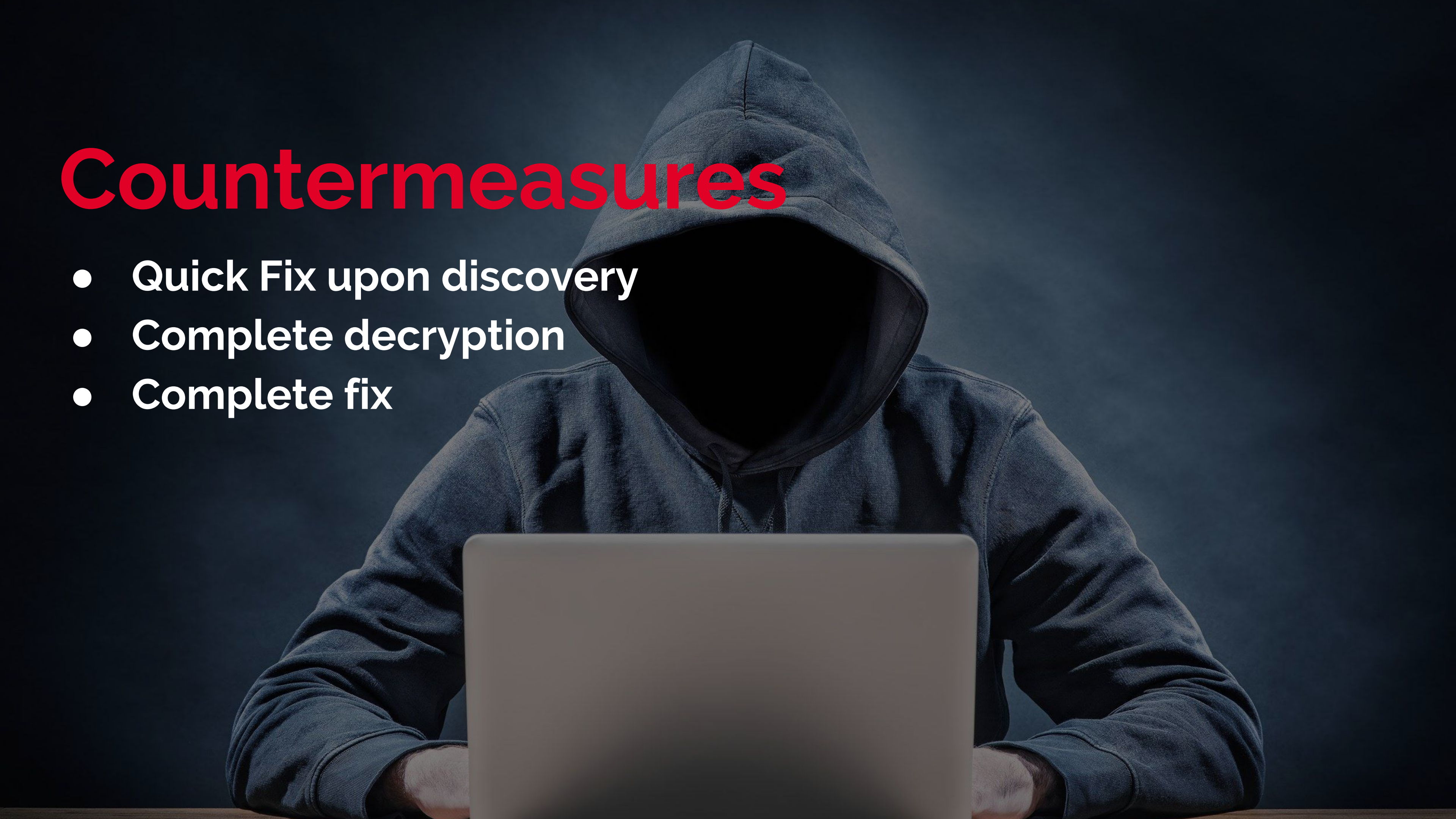
- 549 Likes
- 150 comments
- Unilateral Praise

Stay Alert

- Keep the subject alive
- Find interesting angles
- Use simple language
- If a kitten can do it, so can you



Original connection
User
Internet
New connection
Man in the Middle



Countermeasures

- Quick Fix upon discovery
- Complete decryption
- Complete fix

Your readers are not stupid. They just don’t know anything about the topic yet.

What We Do

- Inform users periodically
- Make knowledge public
- Have a dedicated mail opening service for dodgy-looking mails

What You Can Do

- Keep it simple
- Keep it short
- Keep it alive
- Make your readers feel like they are smart
- Tell a great story

Thank You!