

# Companies like yours

Jan-Jan Lowijs, Maarten Aertsen



DDMA - Datasecurity congres

May 19th, 2015  
Edel, Amsterdam

## Maarten Aertsen



**Privacy team**  
**Deloitte Risk Services**  
**The Netherlands**

Consultant

- Privacy Advisor
- Security Engineer

## Jan-Jan Lowijs



**Privacy team**  
**Deloitte Risk Services**  
**The Netherlands**

Manager

- Privacy & Data protection
- Vulnerability management

## Security & Privacy at Deloitte in the Netherlands

- Over 120 Security & Privacy professionals
- Over 65 CISSP's
- Over 40 Ethical hackers
- Official security and privacy trainers recognized by ISACA, (ISC)<sup>2</sup>, IAPP



On September 19th 2013 the 3rd finals took place in Atlanta. Over 600 teams participated in the preliminary rounds. The 10 best teams representing all continents participated in the finals. The Deloitte Netherlands team won this final for the third time.

# Trends

## The cyber world is ever evolving

### Society & Economy

1. Dependence on technology is growing
2. Connectivity increases dramatically
3. Disruptions in technology are a clear and present danger to business continuity



Cloud computing, Social Media, mobile computing, BYO, remote working, always online, digital-supply-chain, online shopping, online banking, etc.

### Cyber Threats

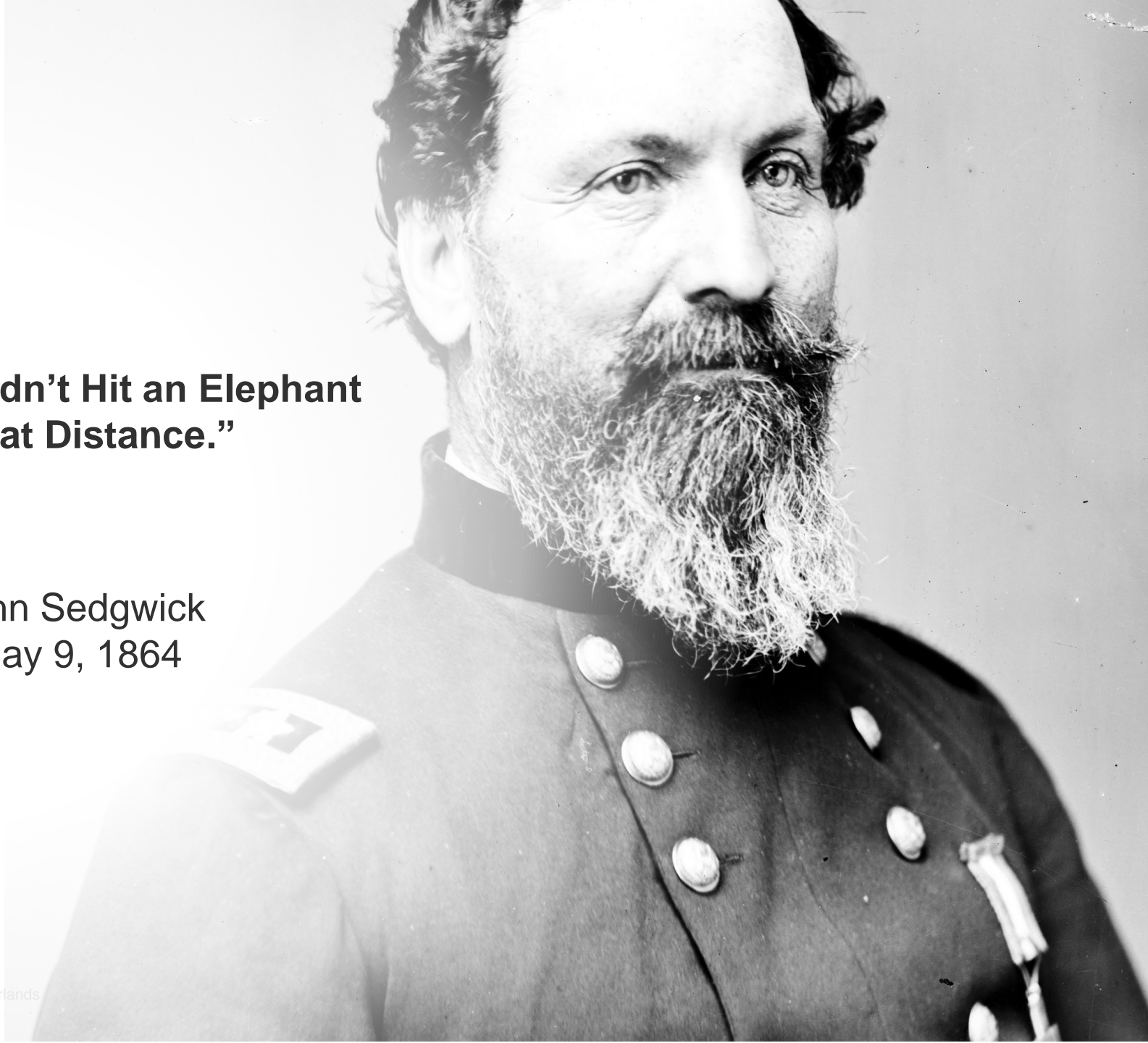
1. Increased digital
2. Cybercrime is professionalizing
3. Increase in other factors and motivations



DDoS, Skimming, SPAM, Phishing, Spear-phishing, Internet banking hack, Credit card data theft, Identity theft, Password cracking, Disclosure confidential data, hacking Social Media, hacking parking terminals, disruption manufacturing systems, etc.

**“They Couldn’t Hit an Elephant  
at that Distance.”**

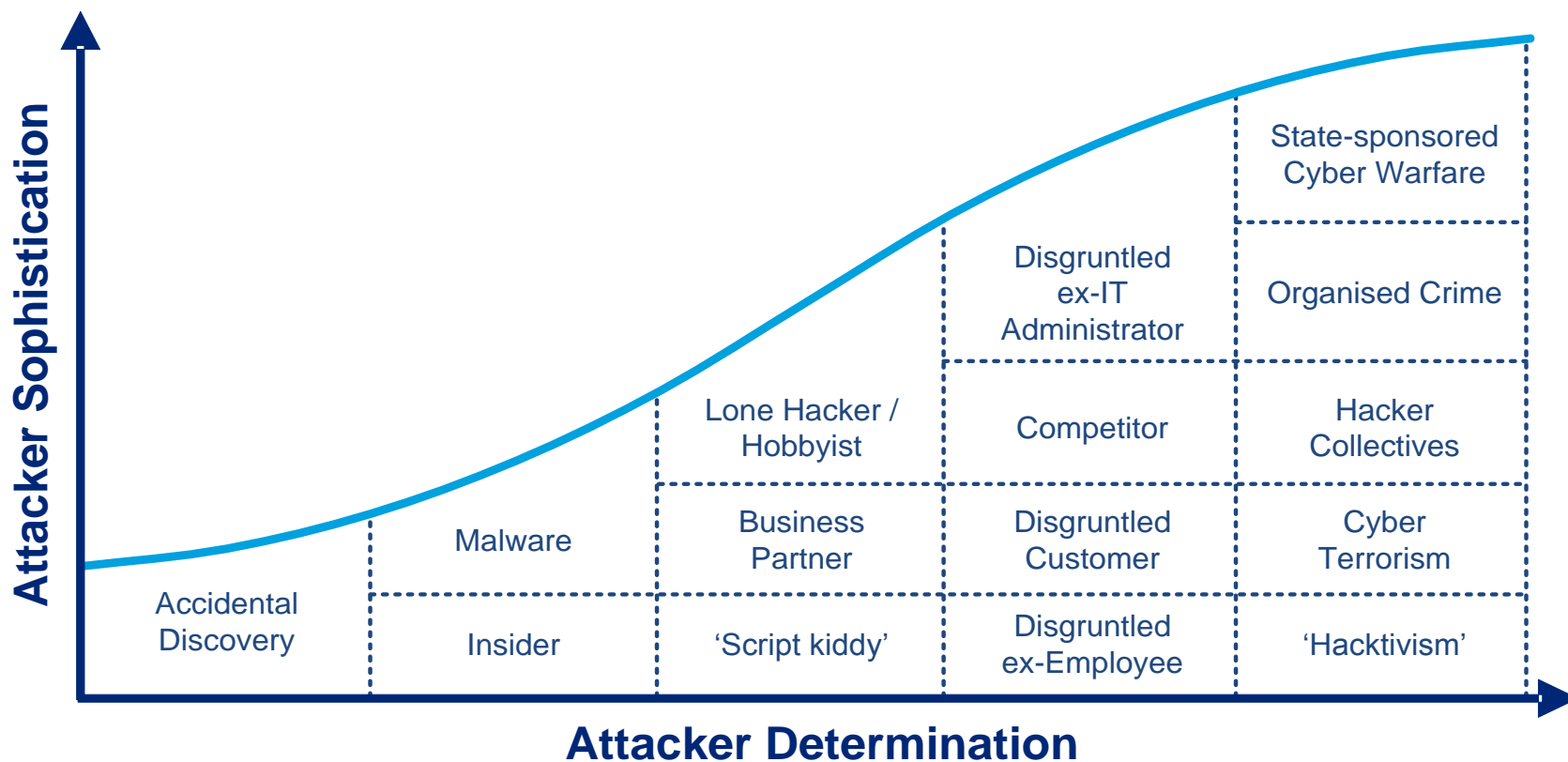
John Sedgwick  
May 9, 1864



# The danger

## Who is targeting you?

Type	Permission?	Criminal Intent?
Blackhat	No	Yes
Greyhat	No	No
Whitehat	Yes	No



# Companies like yours

## Video



# Companies like yours

## Video

<http://www.deloitte.nl/cybervideo>

# Companies like yours

## Comments

### **Nice movie, but...**

- This will never happen to us.
- Not at our company.
- It's too much 'James Bond'.
- It isn't that easy in real life.
- They are just actors.
- ...

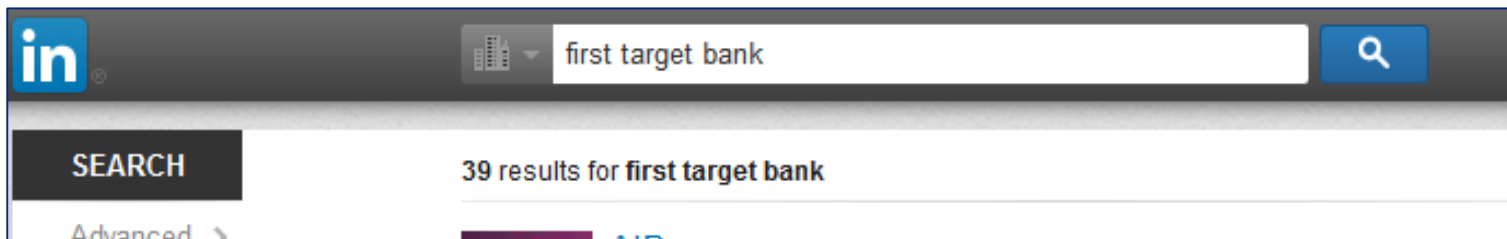
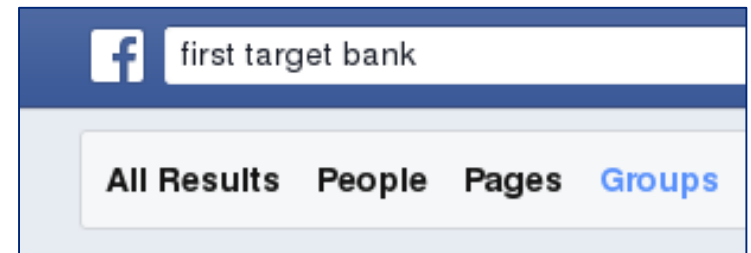


Not in real life?

*Allow us to demonstrate*

# Step 1

## Information gathering



# Step 1

Ally is system administrator.

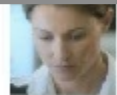


Ally

System administrator at First Target Bank  
The Hague Area, Netherlands

Connect with Ally · 17m ago

Ally expects pictures from Jim.



**Party this Friday!!!**

Hi Jim,

I liked the party pictures you send last week to me. Can you send me the party pictures this friday??



**Jim**

Of course :D 🇳🇱

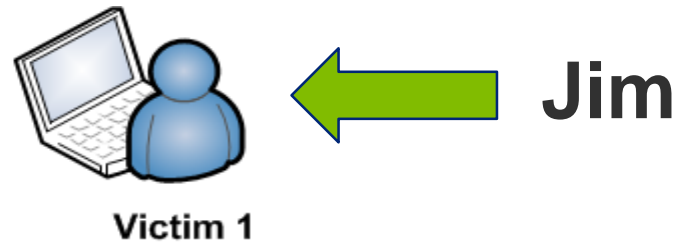
29 minutes ago

# Step 2

## Social engineering



## Step 2

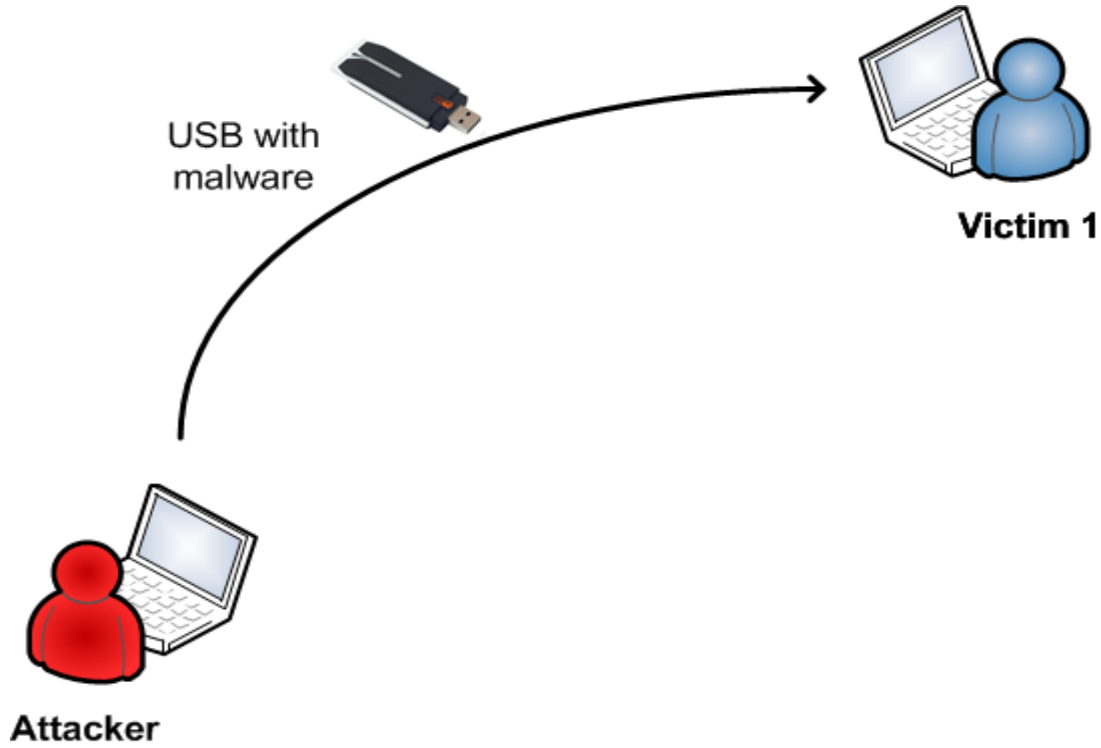


# Step 3

## The infection

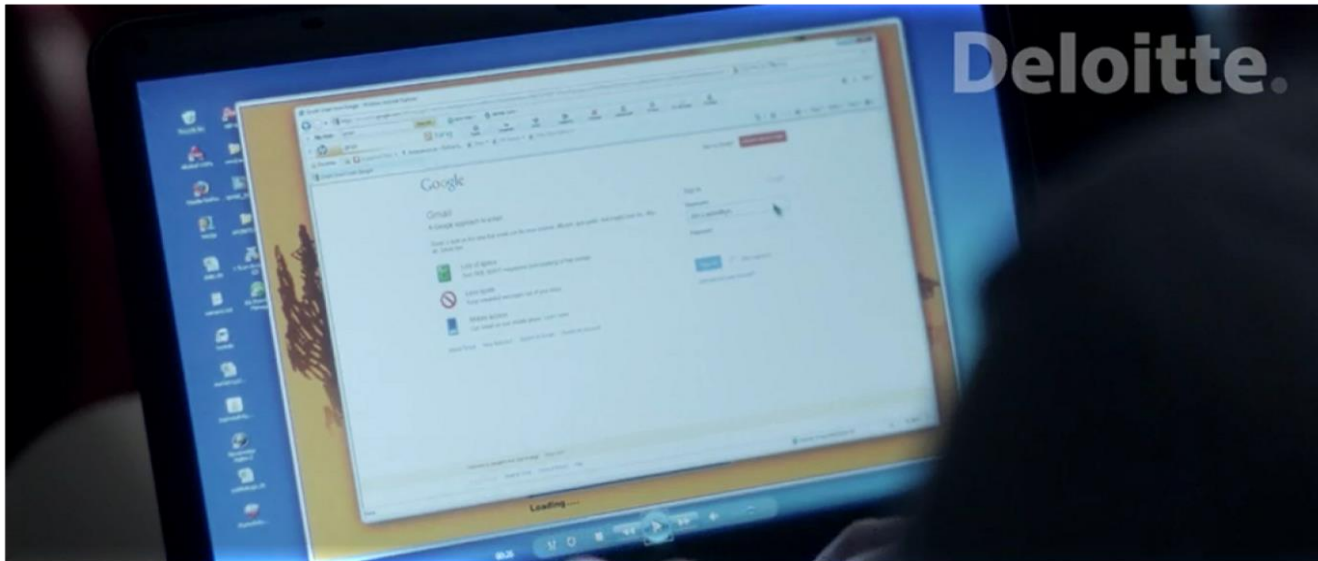


# Step 3



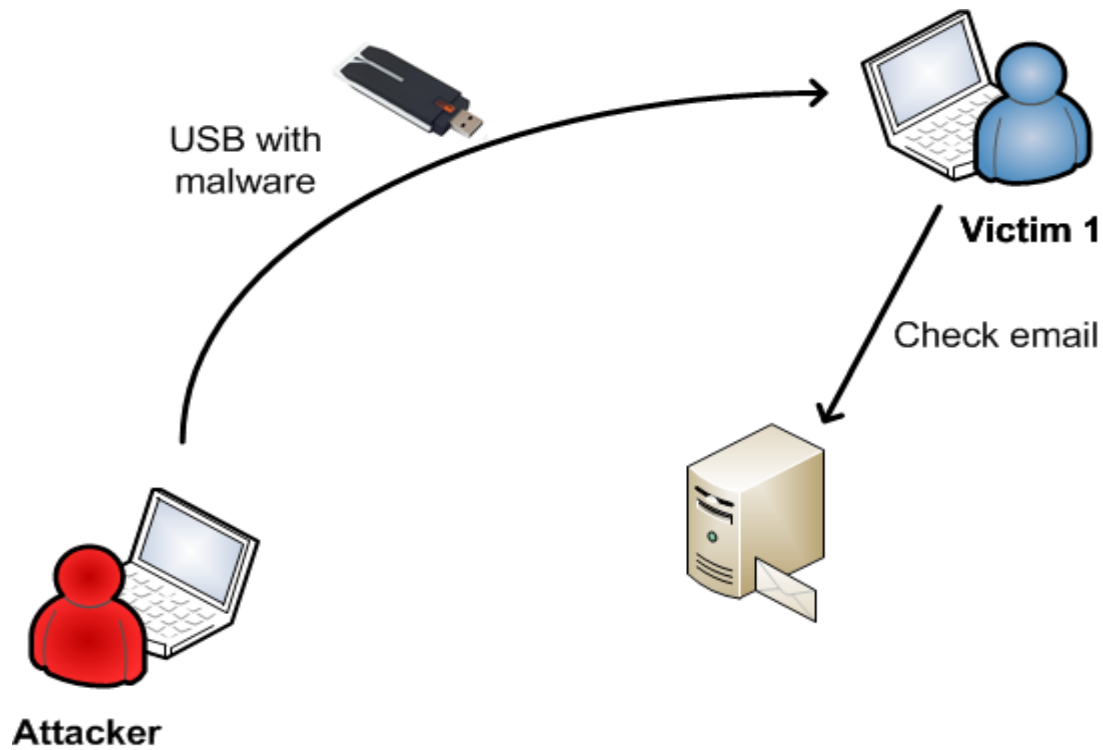
# Step 4

## Gaining access

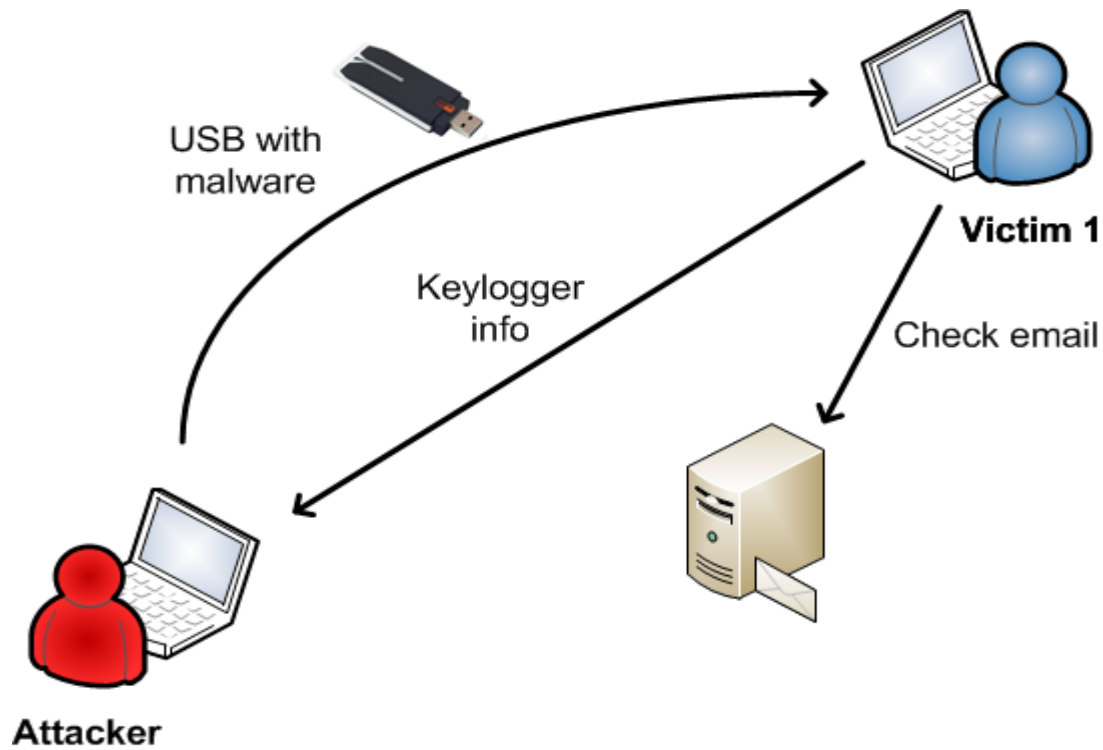




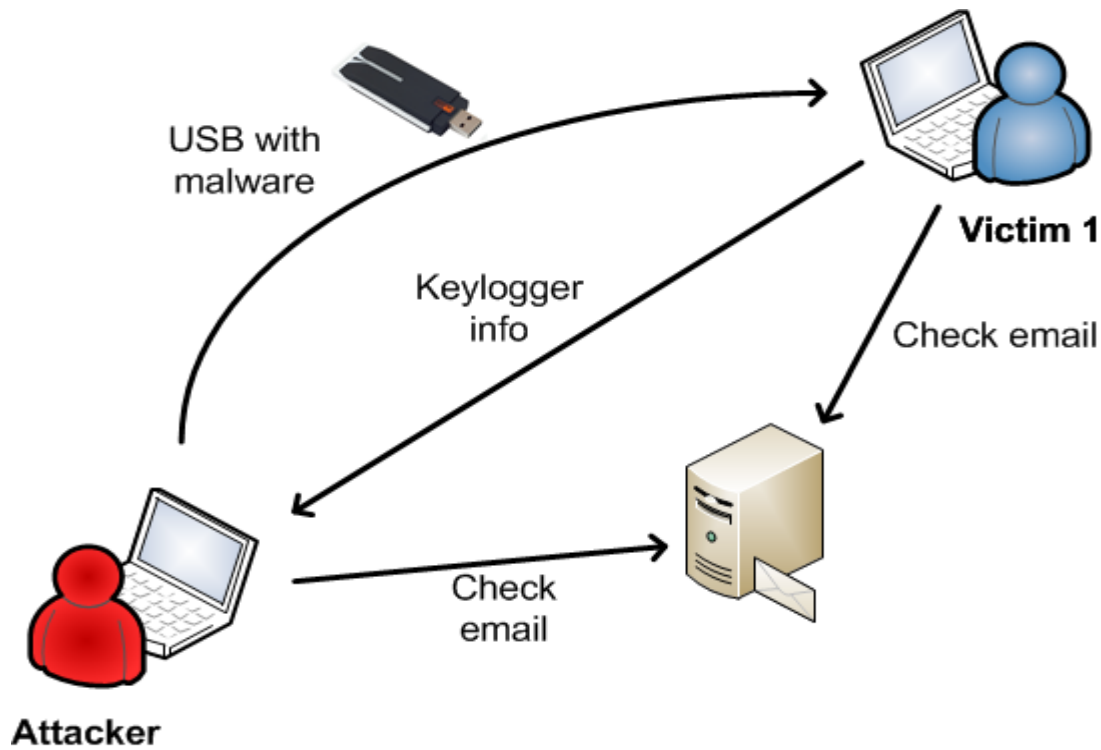
# Step 4



# Step 4

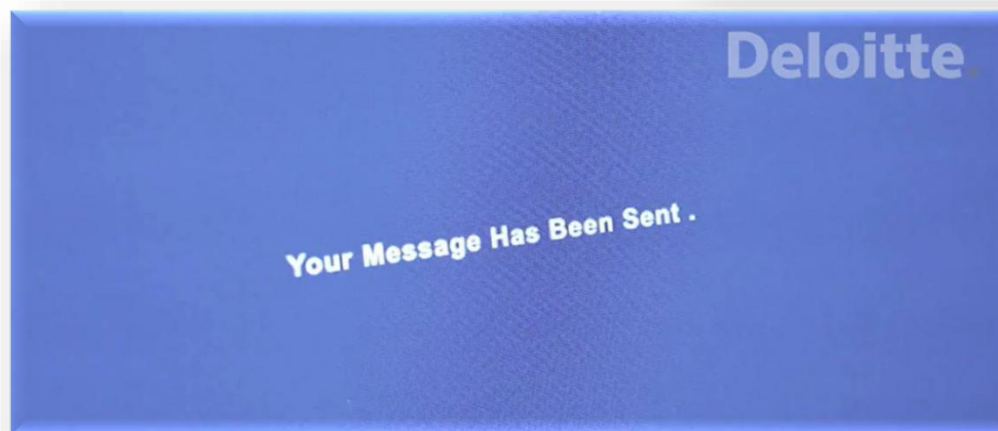
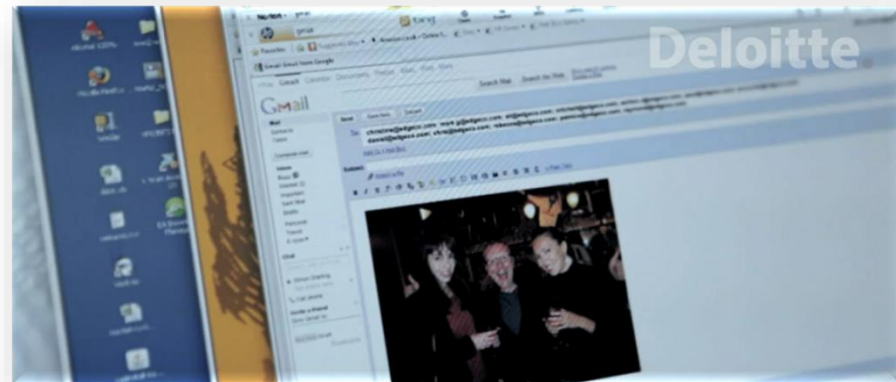


# Step 4

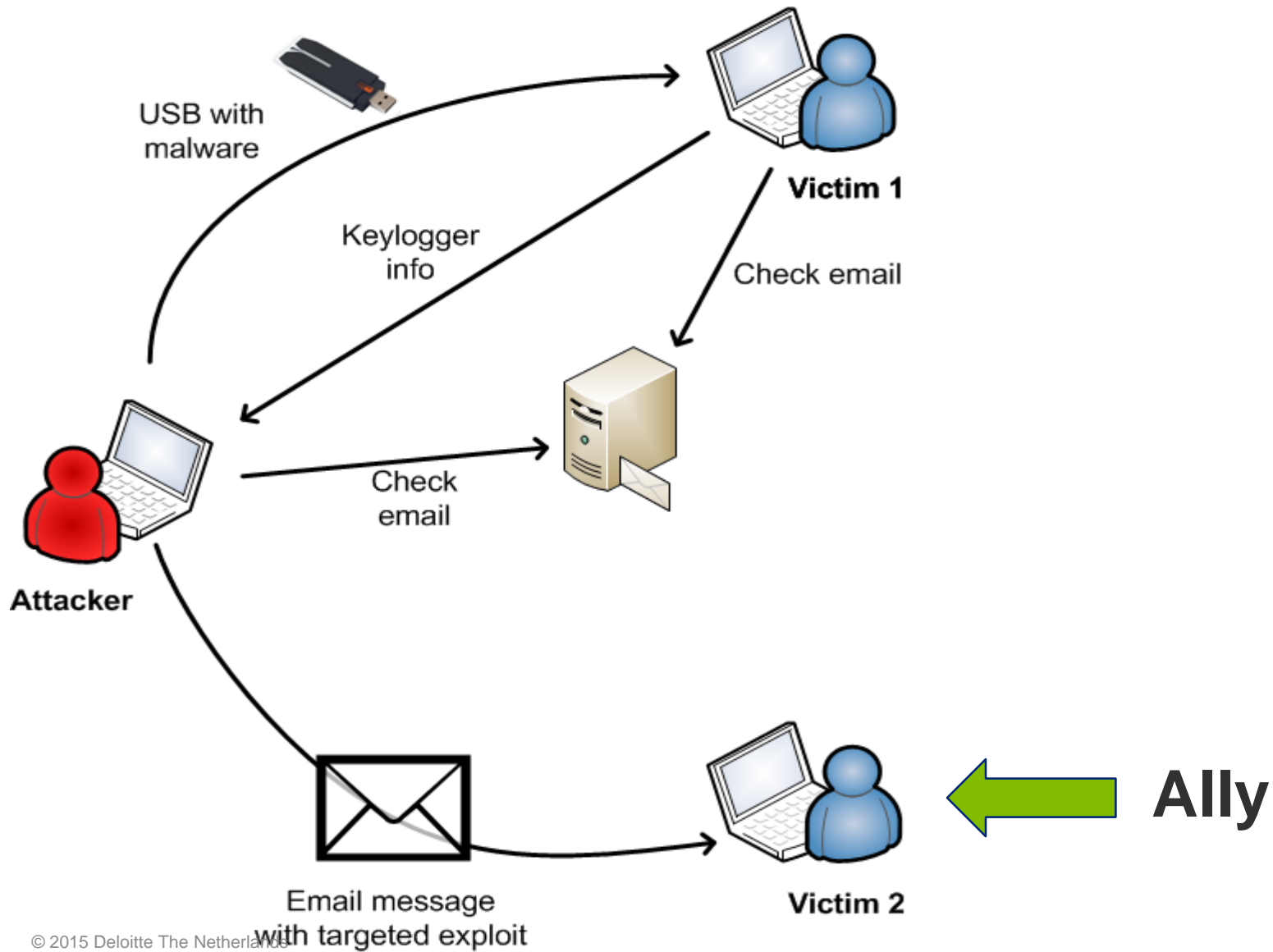


- Access e-mail
- E-mails with passwords
- Password reset option
- Passwords exchange
- Business contacts
- Access LinkedIn
- Access Twitter
- Access Facebook
- Etcetera

# Expanding privileges

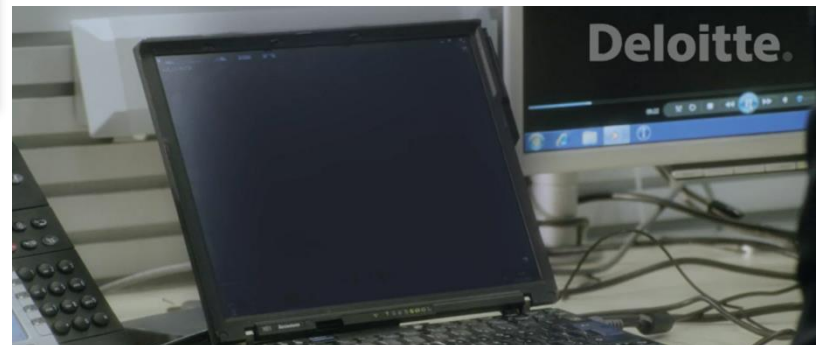
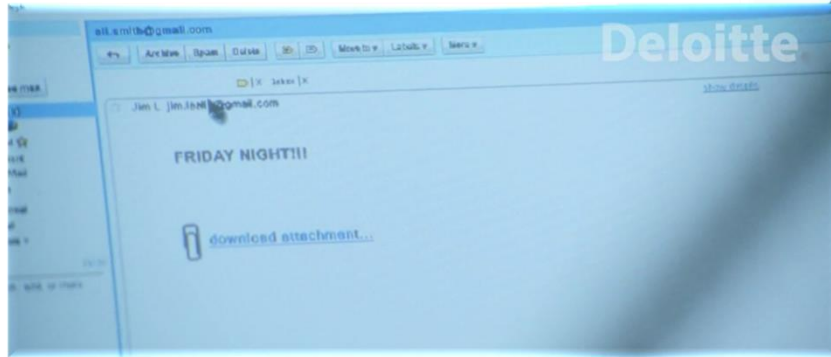


# Step 5

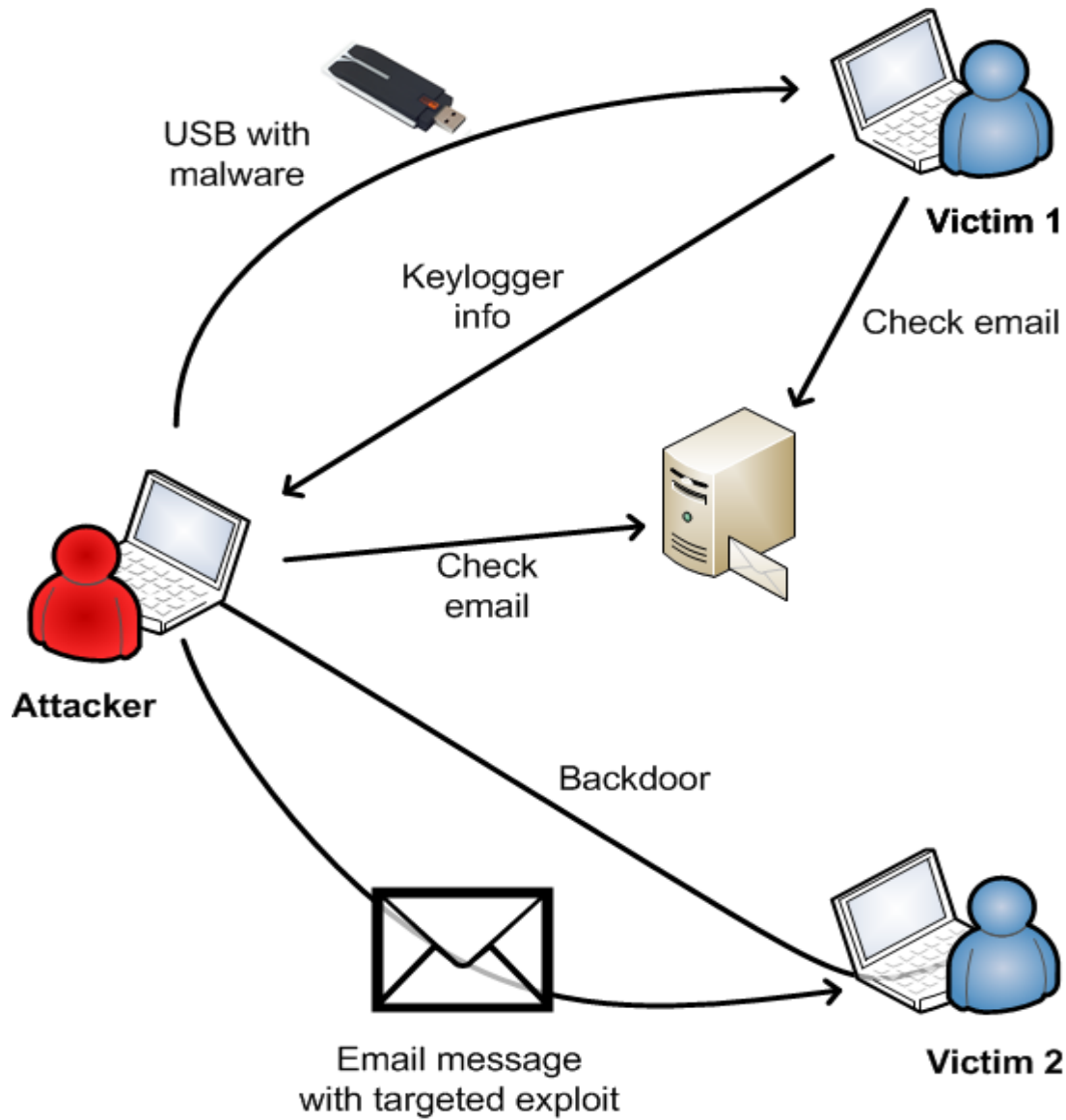


# Step 6

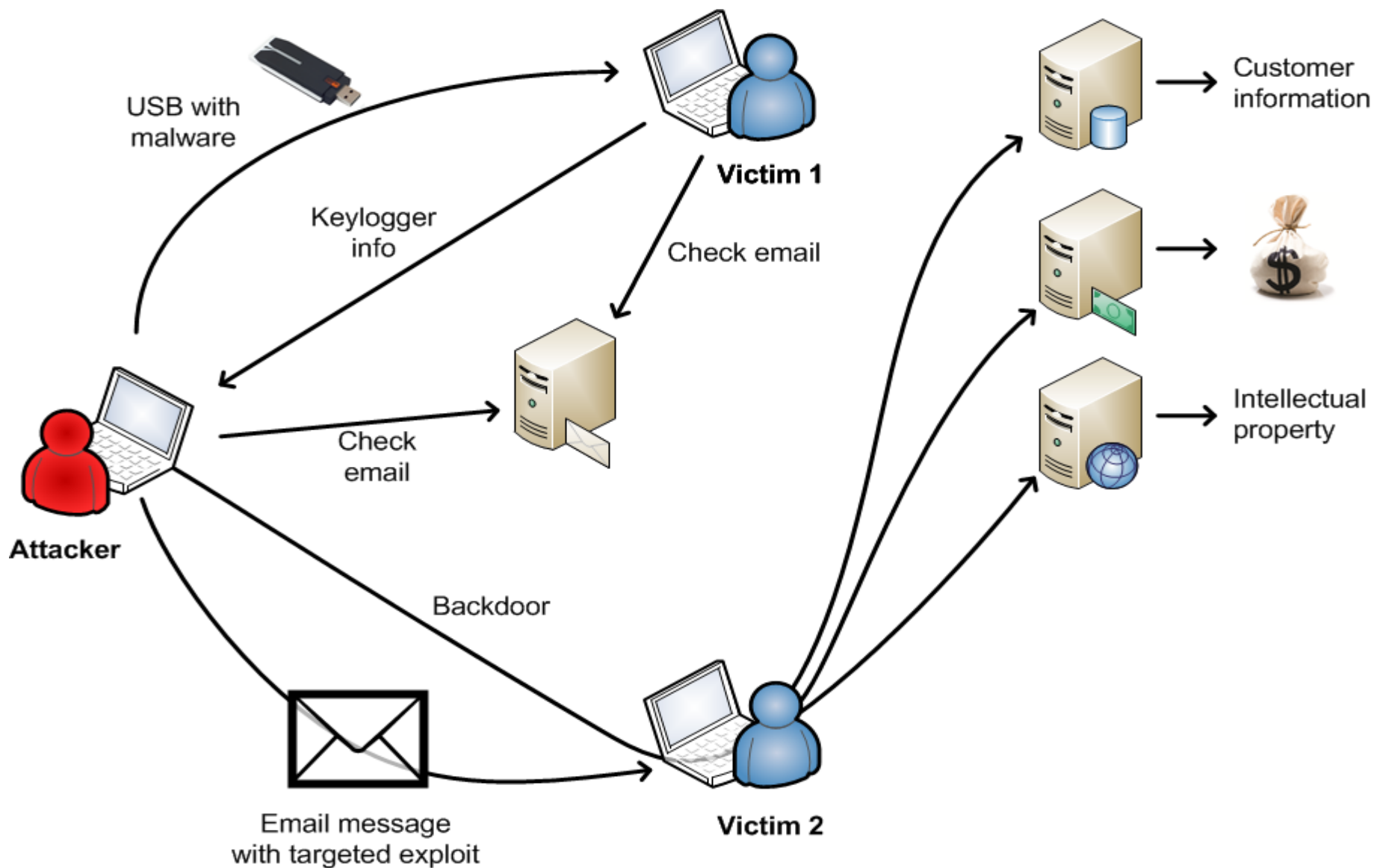
## Taking control



# Step 6



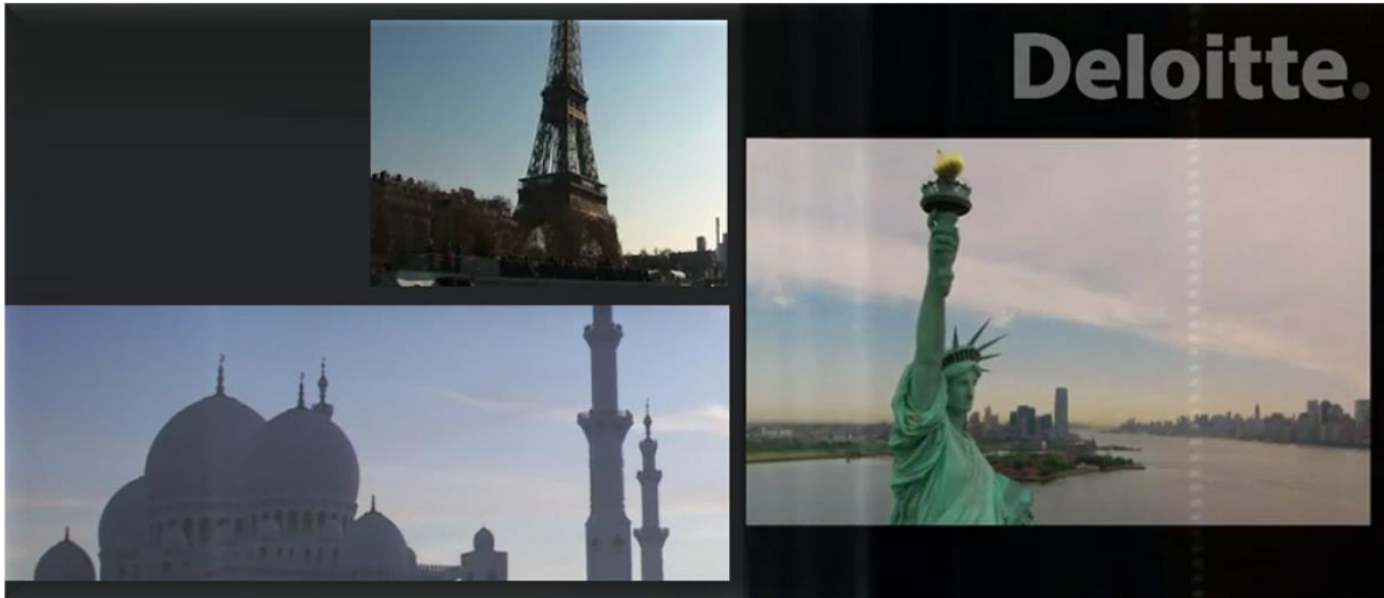
# Step 6



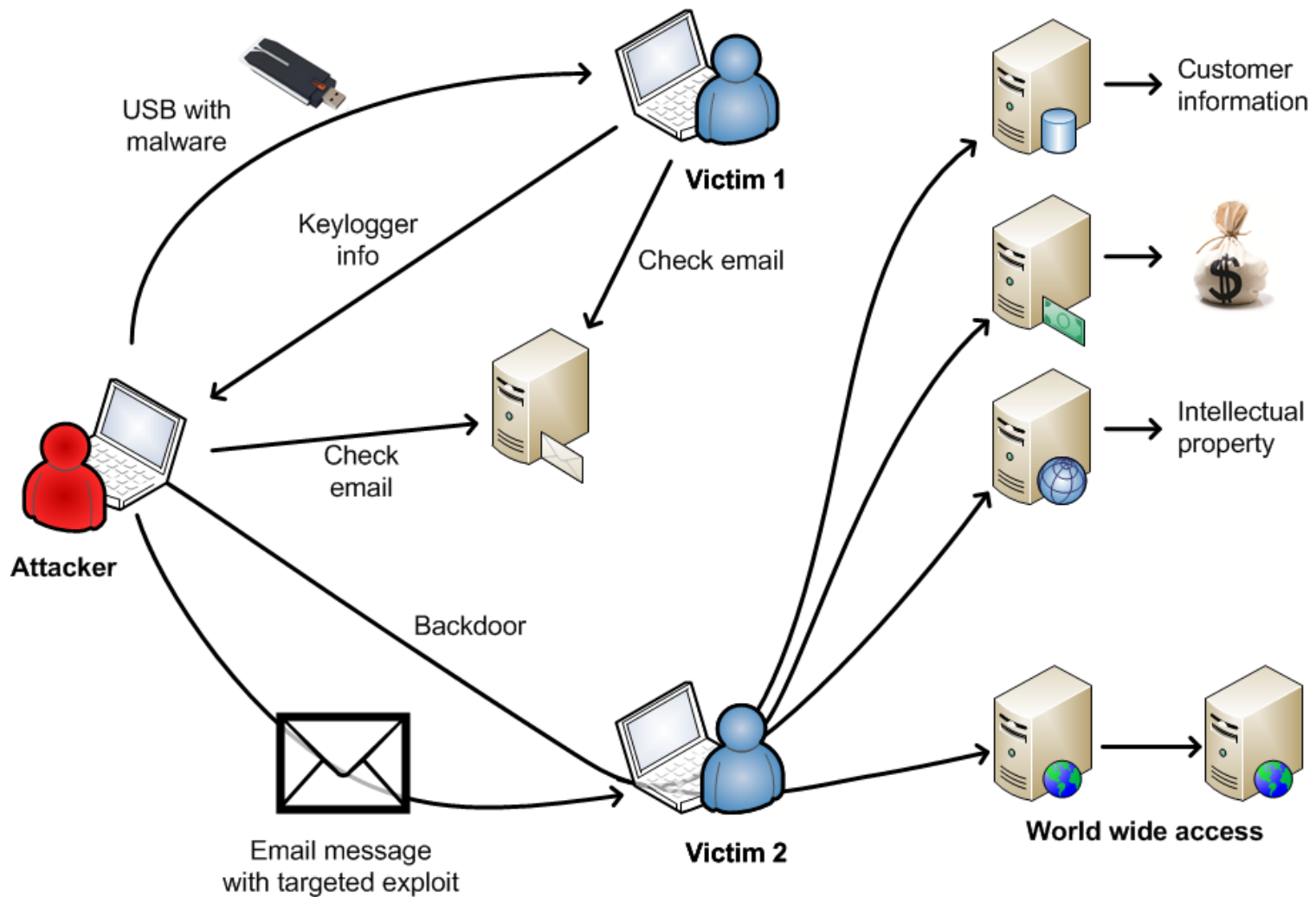


# Step 7

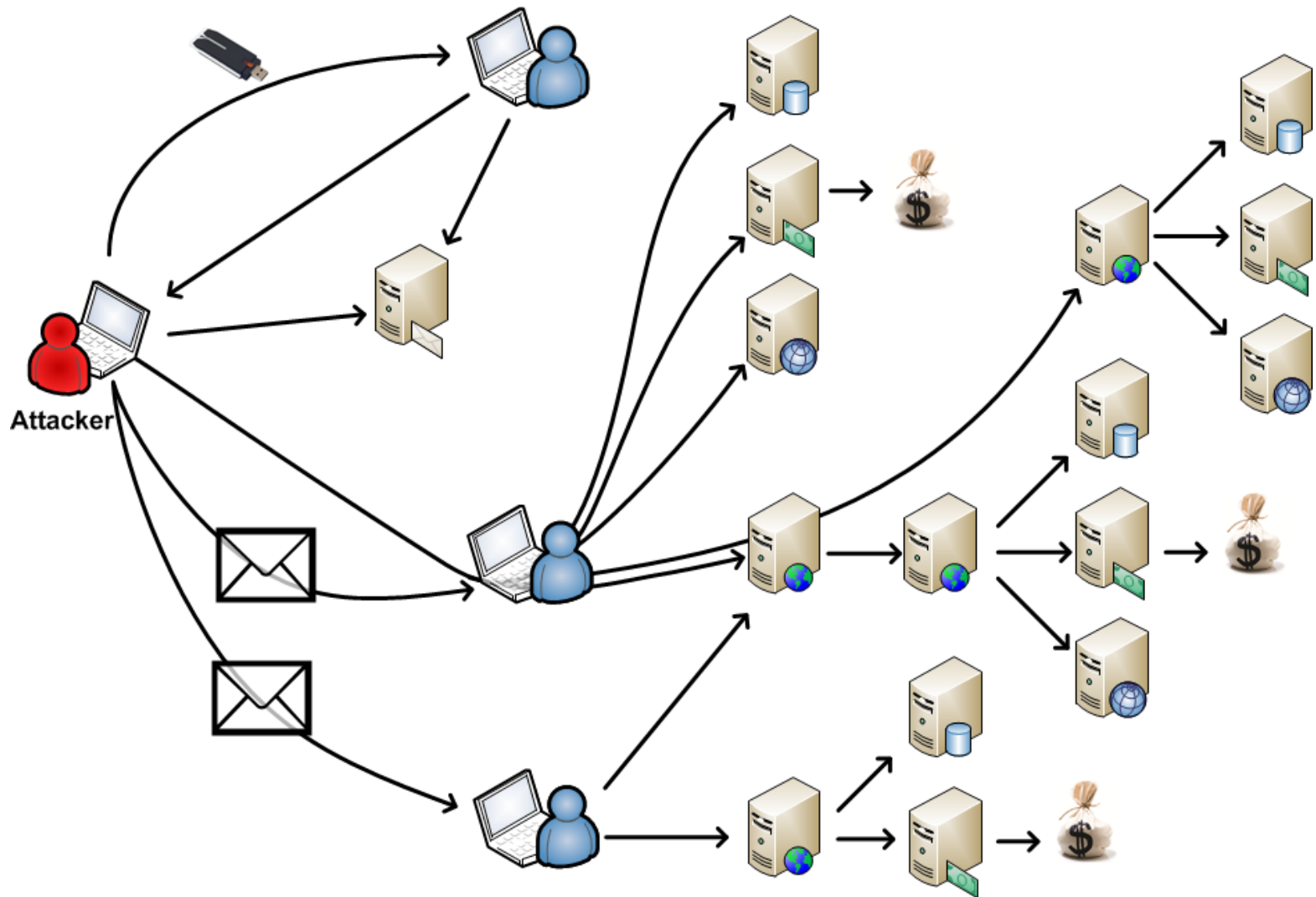
## Worldwide



# Step 7



# Step 7



# Key message

## *Resilience*

# Hackers vs. Defenders

## An asymmetric fight

### Hackers

- Unlimited time, low costs
- Only one hole is sufficient
- Rules do not apply



### Defenders

- Limited time, limited budget
- Time between discovery and mitigation
- Everything is connected and nobody is in charge



**Assume  
you will be  
hacked.**



Hacking.

# Your organization will be breached

## How to respond?

1. Your organization will be hacked; are you able to detect and respond?
2. Can you justify to your stakeholders whether your organization was in control and has gone through careful decision making process to balance risks, mitigation and costs?
3. Can you respond with:
  - what is going on?
  - were you aware of this risk?
  - what did you do to prevent this from happening?
  - what are you doing to contain it?



# Cyber Resilience Cycle





# Closing remarks

## Q&A

# Q&A





Cyber Risk Services  
Gustav Mahlerlaan 2970  
1040 HC, Amsterdam  
The Netherlands

**Jan-Jan Lowijs**

M: +31 6 20 78 96 78  
E: [jlowijs@deloitte.nl](mailto:jlowijs@deloitte.nl)  
I: [www.prepareforprivacy.nl](http://www.prepareforprivacy.nl)

Member of  
**Deloitte Touche Tohmatsu**



Cyber Risk Services  
Gustav Mahlerlaan 2970  
1040 HC, Amsterdam  
The Netherlands

**Maarten Aertsen**

M: +31 6 83 33 00 50  
E: [maertsen@deloitte.nl](mailto:maertsen@deloitte.nl)  
I: [www.prepareforprivacy.nl](http://www.prepareforprivacy.nl)

Member of  
**Deloitte Touche Tohmatsu**



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.