Manolis (Emmanouil Vasilomanolakis)

When everything fails.

Course plan

- Lecture 1: Intro (**Manolis**, **Carsten**) 30.01
- Lecture 2: **Crypto** essentials (**Carsten**) 06.02
- Lecture 3: **Authentication** (**Manolis**), lab bootcamp (TAs) 13.02
- Lecture 4: **TLS** (**Manolis**) 20.02
- Lecture 5: **Threat detection** (**Manolis**) 27.02
- Lecture 6: Hacking Lab day (**TAs**) – blue team 05.03
- Lecture 7: **IoT security** (**Manolis**) 12.03
- Lecture 8: **WIFI security** (**Manolis**) 19.03
- Lecture 9: **Private communication** (**Carsten**) 02.04
- Lecture 10: **When everything fails** (**Manolis**) 09.04
- Lecture 11: Hacking Lab day (**TAs**) – red team 16.04
- Lecture 12: Guest lecture (OT security, **Ludwig**) 23.04
- Lecture 13: **Exam preps** (**Carsten, Manolis**) 30.04

Outline

- Carsten – Signal & Onion routing
- Introduction
- Social engineering attacks
- OSINT
- USB dropping and QR code attacks
- Lab exercise

“There exists, for everyone -a sentence, a series of words - that has the power to destroy you.”
Philip K. Dick, VALIS

SOCIAL ENGINEERING

(MAIN SOURCE:
BLACK HAT USA 2018 TALK: *EVERY ROSE HAS ITS THORN THE DARK ART OF REMOTE ONLINE SOCIAL ENGINEERING*)

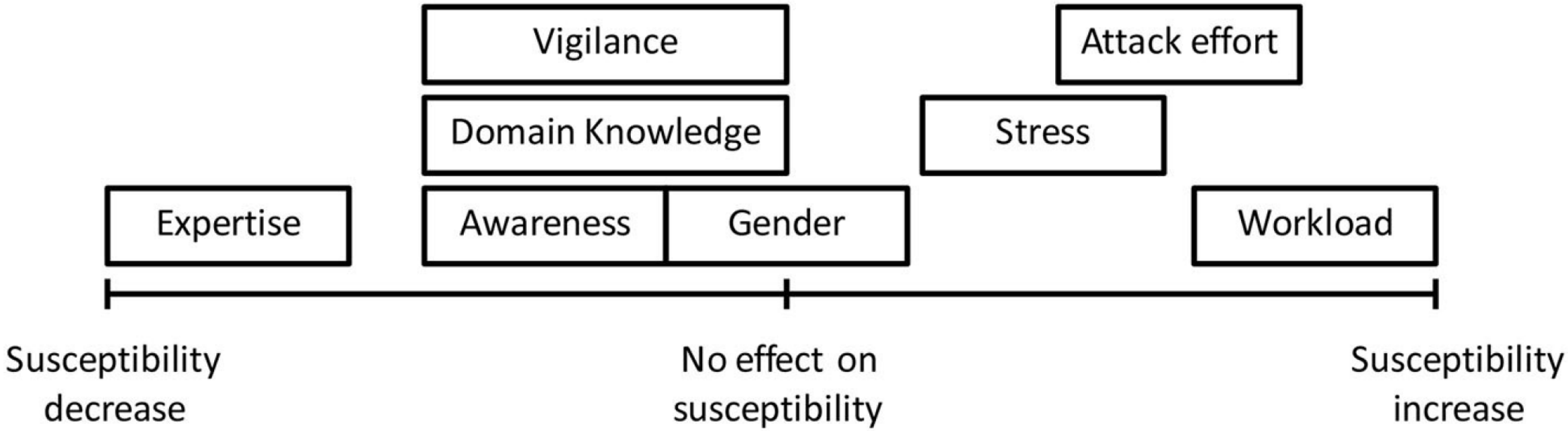
Our focus: remote online social engineering

- But **don't underestimate old school phone call social engineering**

- See: "How to rob a bank over the phone"
  –https://www.youtube.com/watch?v=8n8clT_5bfc

- Or Jim Browning's work:
  https://www.youtube.com/c/JimBrowning

Speculated model on one's susceptibility to social engineering attacks



Online deception types

Trolling

- *The art of trolling* – Matt Joyce, DEF CON 19
- Sophistry & fallacies to provoke responses
- Often used as shorthand for any online abuse

Sockpuppetry

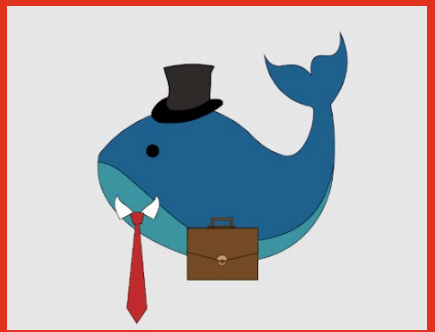
- Often short-term, light on detail
- Posed as independent
- Operated by same entity
- Stealth marketing, false reviews, inflating polls

Astroturfing

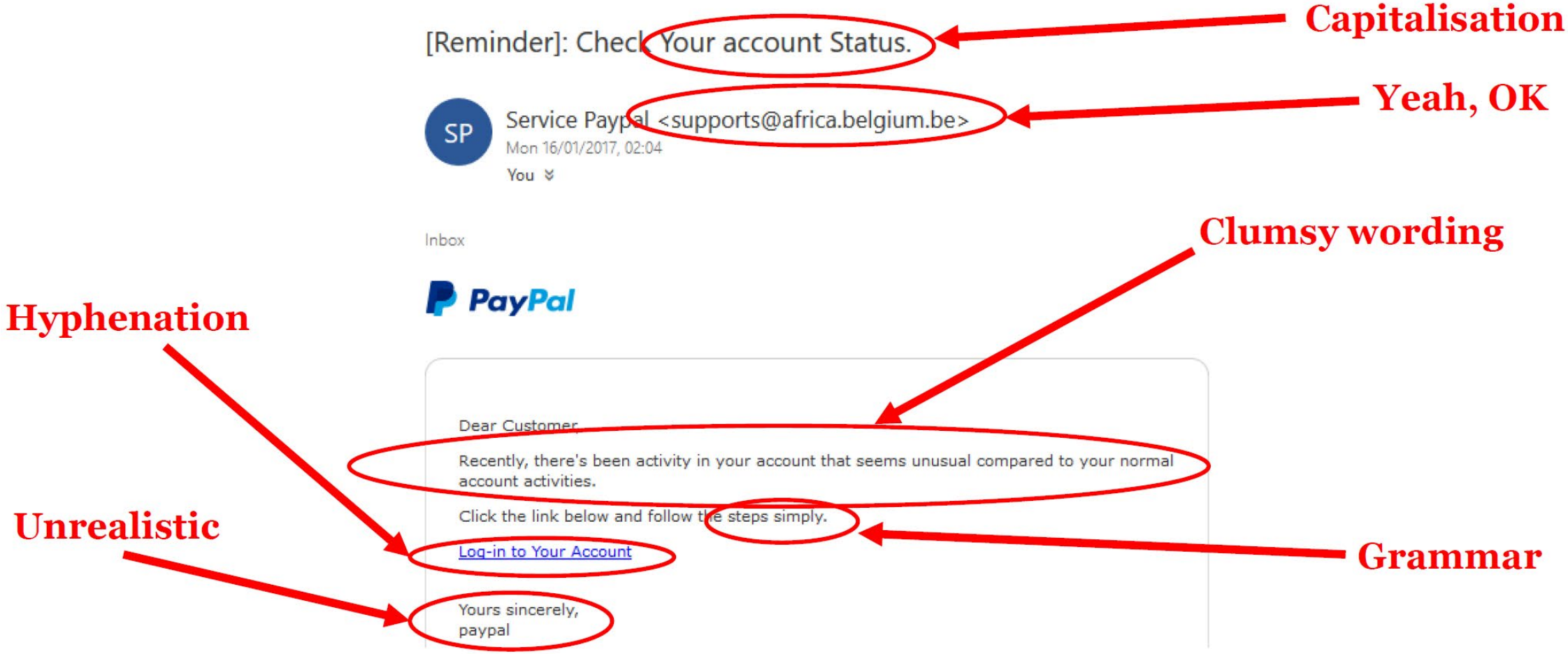
- Sub-category of sockpuppetry
- Used to influence policy, manipulate consensus
  - Especially in politics and marketing
- *Julius Caesar*

Phishing

- Mass phishing
- Spear-phishing
- Whale-phishing



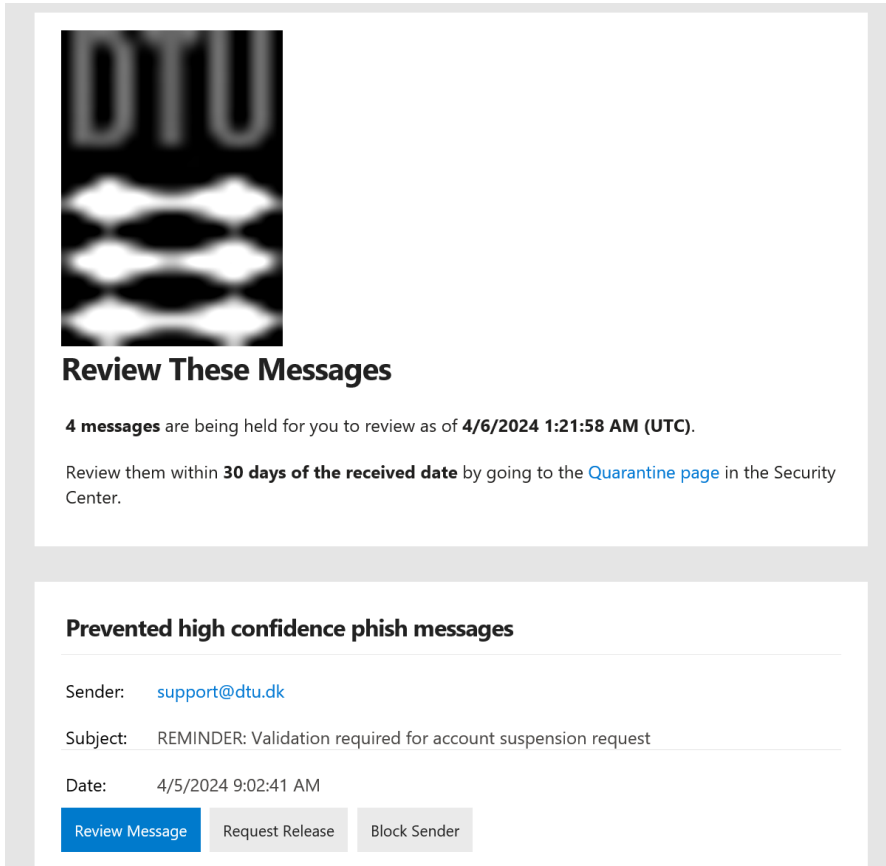
Going beyond mass phishing

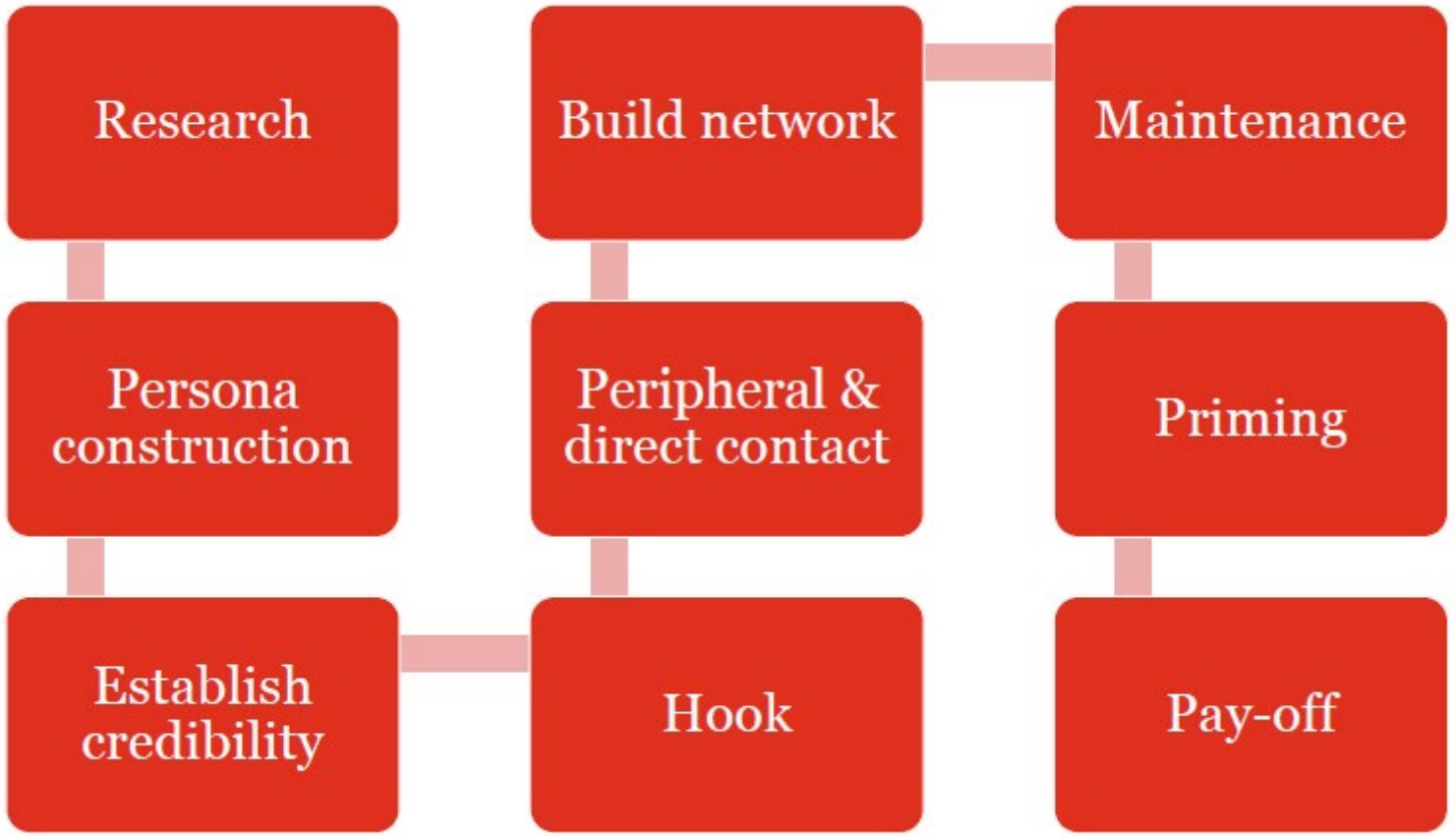


ROSE: REMOTE ONLINE SOCIAL ENGINEERING

Every ROSE has its Thorn: The Dark Art of Remote Online Social Engineering

- Attacks beyond massive phishing
- Goal is to bypass **filters**:
  - Upbringing, education, experience, training, personality
  - Distinctive and consistent (CAPS)
    - Human psychology research
    - Mischel & Shoda , 1995; Michel, 1999; Zayas et al, 2002; Shoda et al, 1994




Research
Persona construction
Establish credibility
Build network
Peripheral & direct contact
Hook
Maintenance
Priming
Pay-off

Research

Attack

- Specific attributes
- Likes/dislikes, interests, hobbies
- Affiliations
- Education/employment
- Relationships and family
- Locations
- Other platforms and profiles
- Purchases, holidays
- Technical info
- Reactions, style, motivations

Defence

- Limit sensitive information
- Google alerts
- Various services to alert when you've been searched for

Persona construction

Attack

- Mirroring or supplementing target
- Similar interests, styles, etc
- Potential openings for contact
- Profile images
  - Not always stolen
  - May be edited/manipulated
  - Or behind paywall or from private source
  - Or completely new

Defence

- Limit sensitive information
- Google alerts and similar
- New additions to network
- Reverse image search
- Manipulation detection
  - Glitches
  - Error level analysis
  - Lighting, textures, patterns, blurs
- Perceptual hashing
- Metadata e.g. dates, and context

Robin Sage case (2010)

- Fake persona
- 25-year-old "cyber threat analyst" at the Naval Network Warfare Command in Norfolk, Virginia.
- She graduated from MIT and had allegedly 10 (!) years of work experience

Robin Sage case (2010)

- 28 days of experiment, 300 connections and friends
- Sage offered consulting work with notable companies Google and Lockheed Martin
- received dinner invitations from several male contacts…

APT groups' personas

- Creating personas seems to be usual business for APT groups
- Example: ITG18 APT
  - Multiple accounts on all major companies (gmail, aol, yahoo, hotmail, etc.)
  - Western names, Iranian phone numbers associated with accounts, ITG18 vpn IP addresses

Establishing credibility

Attack

- Referencing institutions, places, companies, etc
- Backdating – not 100% reliable
- Pre-age accounts: create in advance
  - May auto-post for some time
- Profiles which age over time
  - Change images, styles, politics
- Profiles never used for attacks
  - But their "children" are in 20 years
  - Playing the really long game

Defence

- New accounts are suspect
- Backdating can be examined
- Check for early auto-posting (anti-bot analysis)
- Validation (direct or indirect)
- Genuine knowledge: attribution
- Inconsistencies: opportunity
- **Share findings**

Building a synthetic network

Attack

- Proxies, Tor, burner phones, SIM swapping, etc
- More advanced techniques
  - Deepfakes
  - Voice morphing
  - Google Duplex
- Avoiding profile contamination
- Distinctive voices and styles

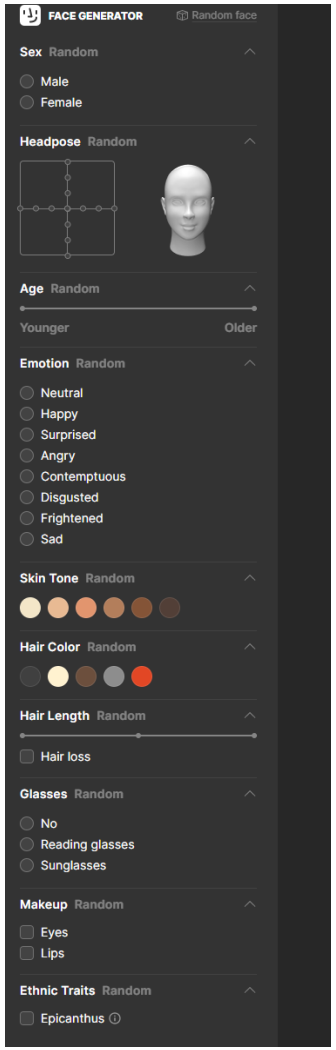
Defence

- Forensic linguistics
- Behavioural attribution
- Check for profile contamination
- Inconsistencies
- Cultural indicators
- Metadata

Example of completely new images…

No worries, AI is here for you:

- https://thispersondoesnotexist.com/
- https://generated.photos/



Peripheral & direct contact

Attack

- Starting with associates
  - Shows on feed = context later
- 'Like' same things
- Trying to get into circle of awareness
- cp. *Donnie Brasco* (Pistone, 1988)
- Liking, commenting, adding
- Prefaced w/ reference to peripheral

Defence

- Corroborate with mutual associates

Silk road case

- Persona creation, fake murders, etc.
  - See https://arstechnica.com/tech-policy/2015/02/the-hitman-scam-dread-pirate-roberts-bizarre-murder-for-hire-attempts/

The hook

Attack

- Informed by earlier research
- Could be request for help/advice
- Or something that will benefit
  - Flirting/sexual
  - Business relationships
  - Ambitions/fantasies
- Shift to corporate email
- Reveals background subtly
  - Drip-feed basis

Defence

- Self-assessment
- Understanding your filters
  - Self-assessment of flaws
- Question motivations and consequences
- Ask how corporate email was found
- Question why they want to shift to corporate email
- Consider ‘sandboxing’ on social media

Maintenance

Attack

- Frequent contact
- Adapted to reality e.g.
  - Local holidays and events
  - Office hours, timezones
  - Appropriate IP and geolocation
- Adapts to responses and context
- Building rapport and trust
- Draws target into synthetic web
  - Use other profiles to communicate
  - Insurance
  - Other angles and opportunities

Defence

- Forensic linguistics
- Behavioural attribution
- Check for evasiveness around voice/video/F2F comms
- Inconsistencies and errors

Priming

Attack

- Microcosm
  - e.g. multiple benign attachments
  - or revealing less valuable info
  - or clicking on links
- Obtains technical feedback
- Conditioning
- Small steps to bigger ones

Defence

- Question motivations when asked to do something
- Qs on technical aspects = red flag

The pay-off

Attack

- Launches attack
  - Attachment
  - Link
  - Ask for information
  - Extortion
  - Seed profile with malware
- May maintain contact
  - To re-use profile in future
  - Now with real-world corroboration
- Or may disappear

Defence

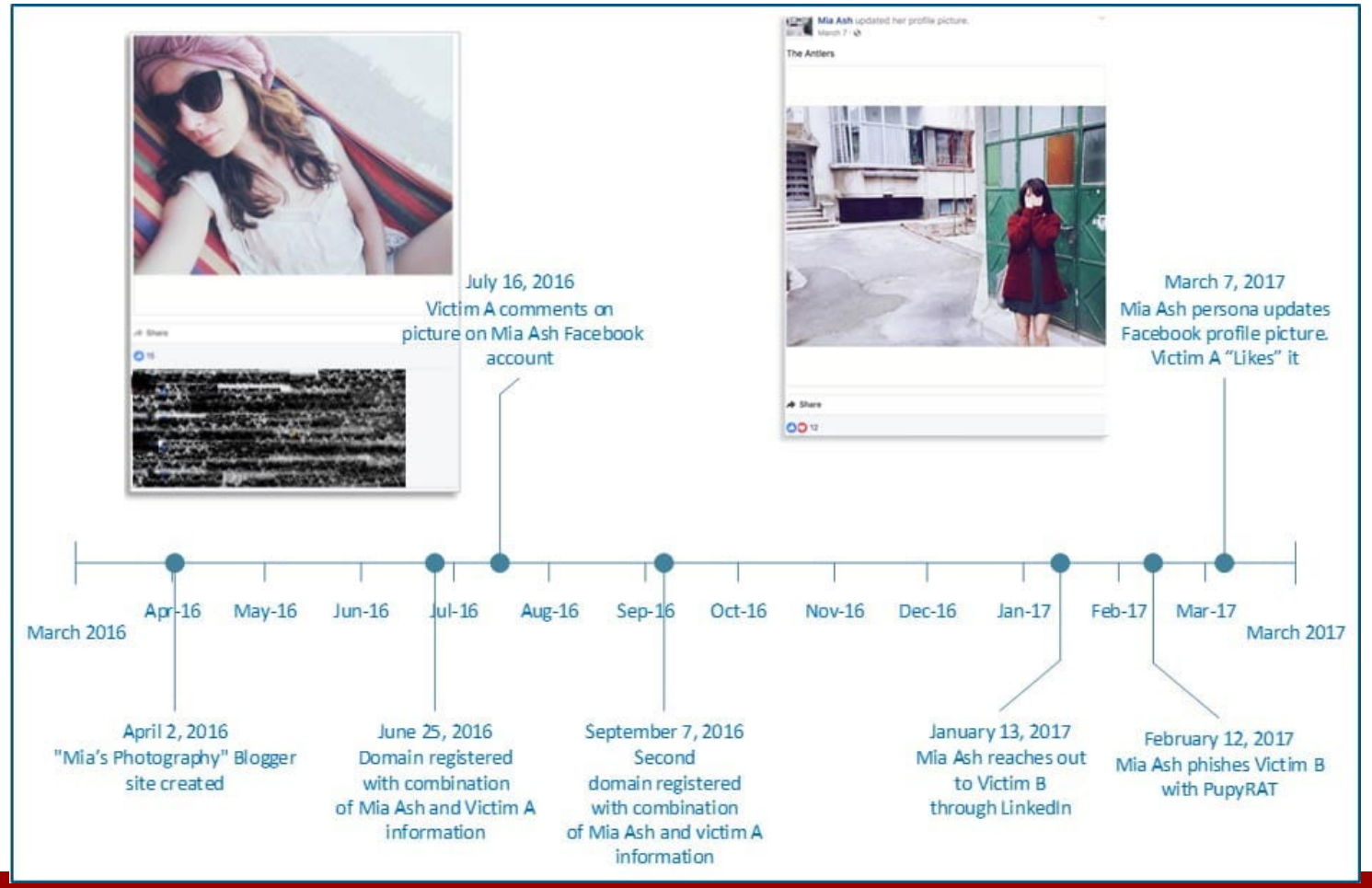
- Sudden disappearance or lack of contact/interests = red flag

Mia Ash case (2017)

- At least 1 year of fake profile creation
- London photographer
- Targets:
  - Saudi Arabia, United States, Iraq, Iran, Israel, India, and Bangladesh
  - worked for technology, oil/gas, healthcare, aerospace, and consulting organizations
  - mid-level employees in technical or project management roles with job titles such as technical support engineer, software developer, and system support

Mia Ash case (2017)

- Further reading: https://www.secureworks.com/research/the-curious-case-of-mia-ash



The VERY recent XZ backdoor case (2021-2024)

Outline

- Carsten – Signal & Onion routing
- Introduction
- Social engineering attacks
- OSINT
- USB dropping and QR code attacks
- Lab exercise

Open-source intelligence (OSINT)

OSINT: powerful tool for defenders & attackers

- OSINT is an umbrella term to describe *the* ***collection and analysis of data gathered from open sources to produce actionable intelligence***

- Open sources can be a lot of things:
  - Social media
  - Public government data
  - Media (e.g., newspapers, TV)
  - Search engine data mining
  - Internet archiving websites
  - Etc.

Google dorking

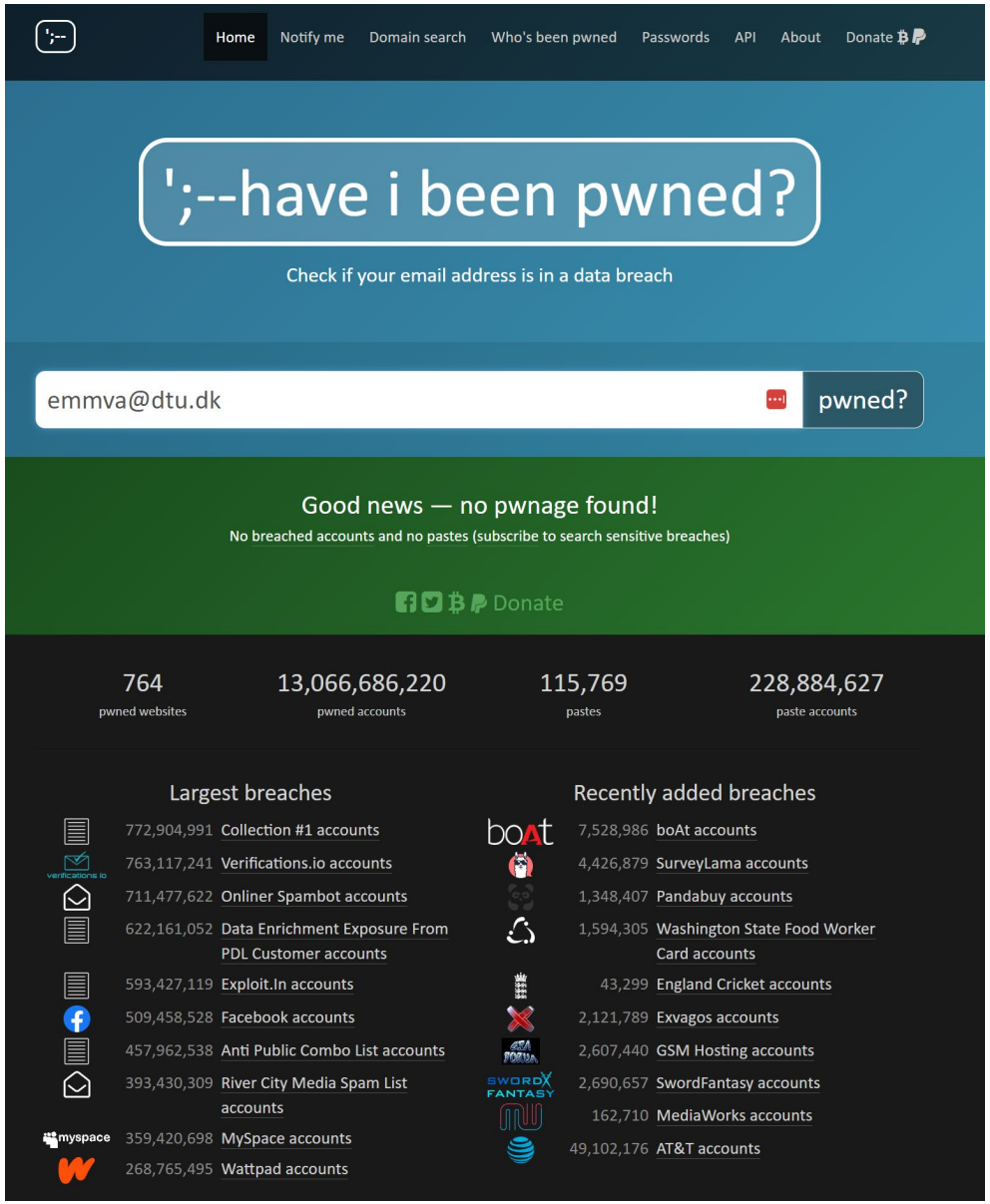
- Google dorking is the art of using complex (or not) queries using Google's filters
- This can have devastating effects for your network/accounts/websites
- In a few seconds one can find:
  - Leaked password data
  - Credit card details
  - Vulnerable websites
  - Web cameras
  - Etc.

Search filters

Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	`allintext:"keyword"`
intext	Searches for the occurrences of keywords all at once or one at a time.	`intext:"keyword"`
inurl	Searches for a URL matching one of the keywords.	`inurl:"keyword"`
allinurl	Searches for a URL matching all the keywords in the query.	`allinurl:"keyword"`
intitle	Searches for occurrences of keywords in title all or one.	`intitle:"keyword"`
allintitle	Searches for occurrences of keywords all at a time.	`allintitle:"keyword"`
site	Specifically searches that particular site and lists all the results for that site.	`site:"www.google.com"`
filetype	Searches for a particular filetype mentioned in the query.	`filetype:"pdf"`
link	Searches for external links to pages.	`link:"keyword"`
numrange	Used to locate specific numbers in your searches.	`numrange:321-325`
before/after	Used to search within a particular date range.	`filetype:pdf & (before:2000-01-01 after:2001-01-01)`
allinanchor (and also inanchor)	This shows sites which have the keyterms in links pointing to them, in order of the most links.	`inanchor:rat`
allinpostauthor (and also inpostauthor)	Exclusive to blog search, this one picks out blog posts that are written by specific individuals.	`allinpostauthor:"keyword"`
related	List web pages that are "similar" to a specified web page.	`related:www.google.com`
cache	Shows the version of the web page that Google has in its cache.	`cache:www.google.com`

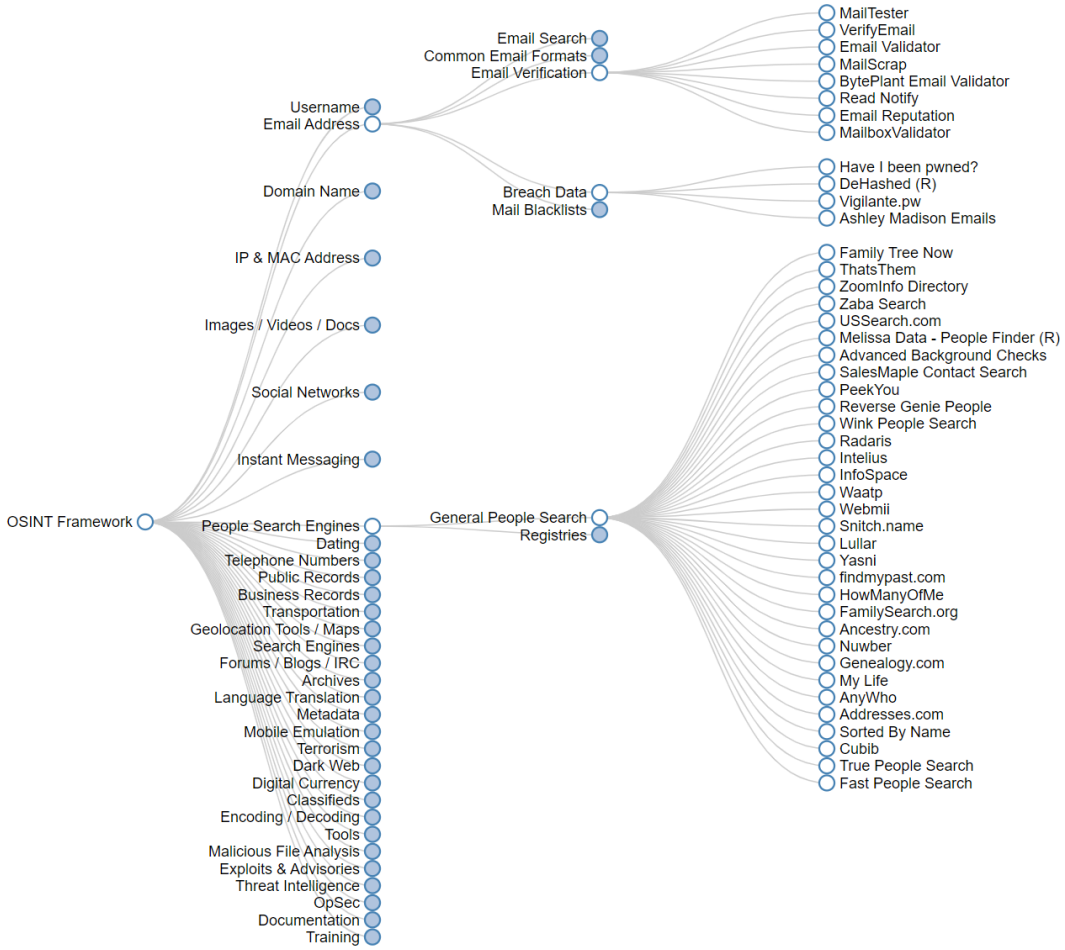
Leaked passwords

- Tools like *have I been pwned?* are great but can also have a dual use
  - –Attacker scanning for your email
  - –Password reusage/recycling
  - –But also profiling (e.g., services used)



Connecting the pieces together: https://osintframework.com

- Collection of multiple sources for OSINT
  - –Quite a few work nicely
  - –Some turned into businesses
  - –Some have expired



Outline

- Carsten – Signal & Onion routing
- Introduction
- Social engineering attacks
- OSINT
- USB dropping and QR code attacks
- Lab exercise

USB dropping

USB dropping attacks

- Three classes of attacks:
  - **Social engineering** (common)
  - **HID spoofing** (very common - this is rubber ducky)
  - **0-day driver exploit** (uncommon)

USB dropping attacks

- Pros & cons per method (source Black Hat USA 2016)

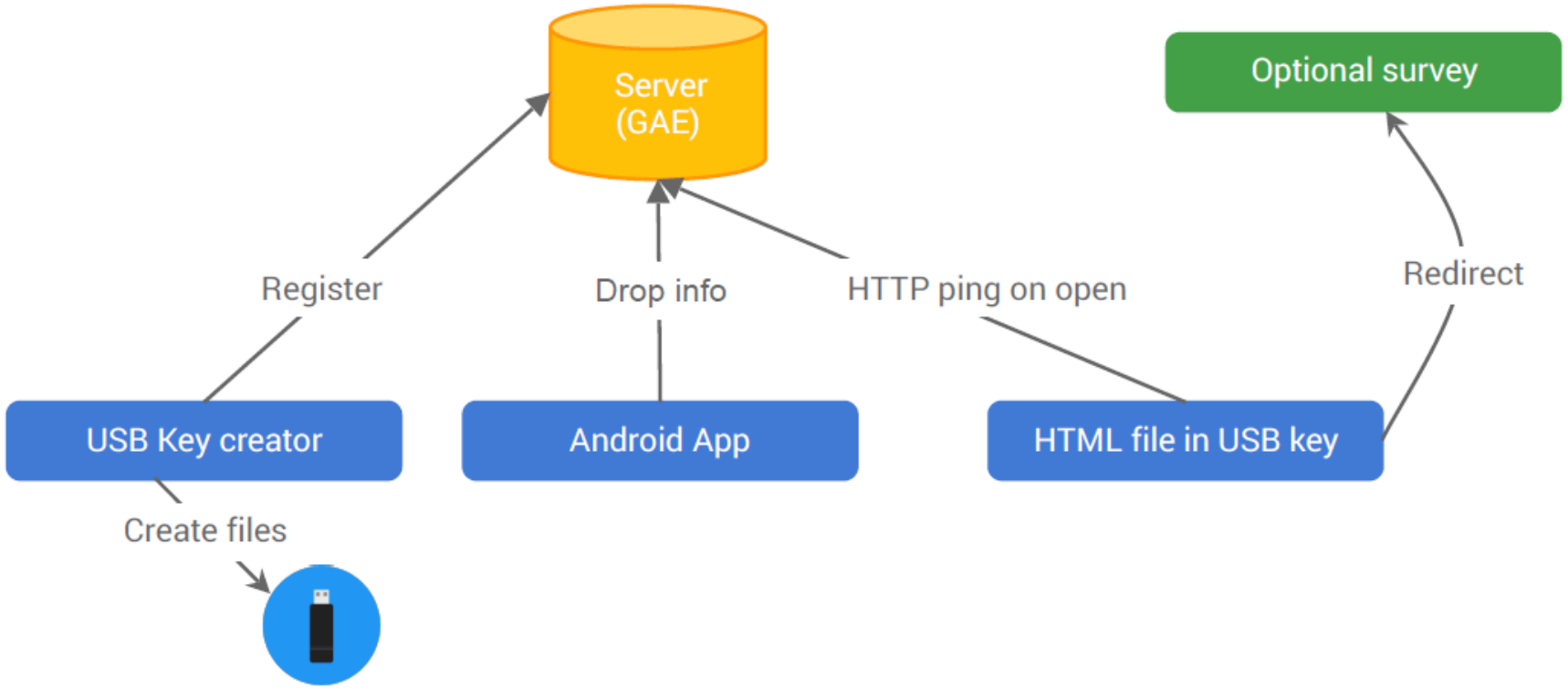
Attack vector	Mostly used by	Complexity & Cost	Reliability	Stealth	Cross OS
Social engineering	Academics Our study!	★	★	★	★★★
HID Spoofing Human Interface Device	White Hat Corporate espionage	★★	★★★	★★	★★
0-day	Government High-end corp espionage	★★★★	★★★★	★★★★	★

USB SOCIAL ENGINEERING ATTACKS

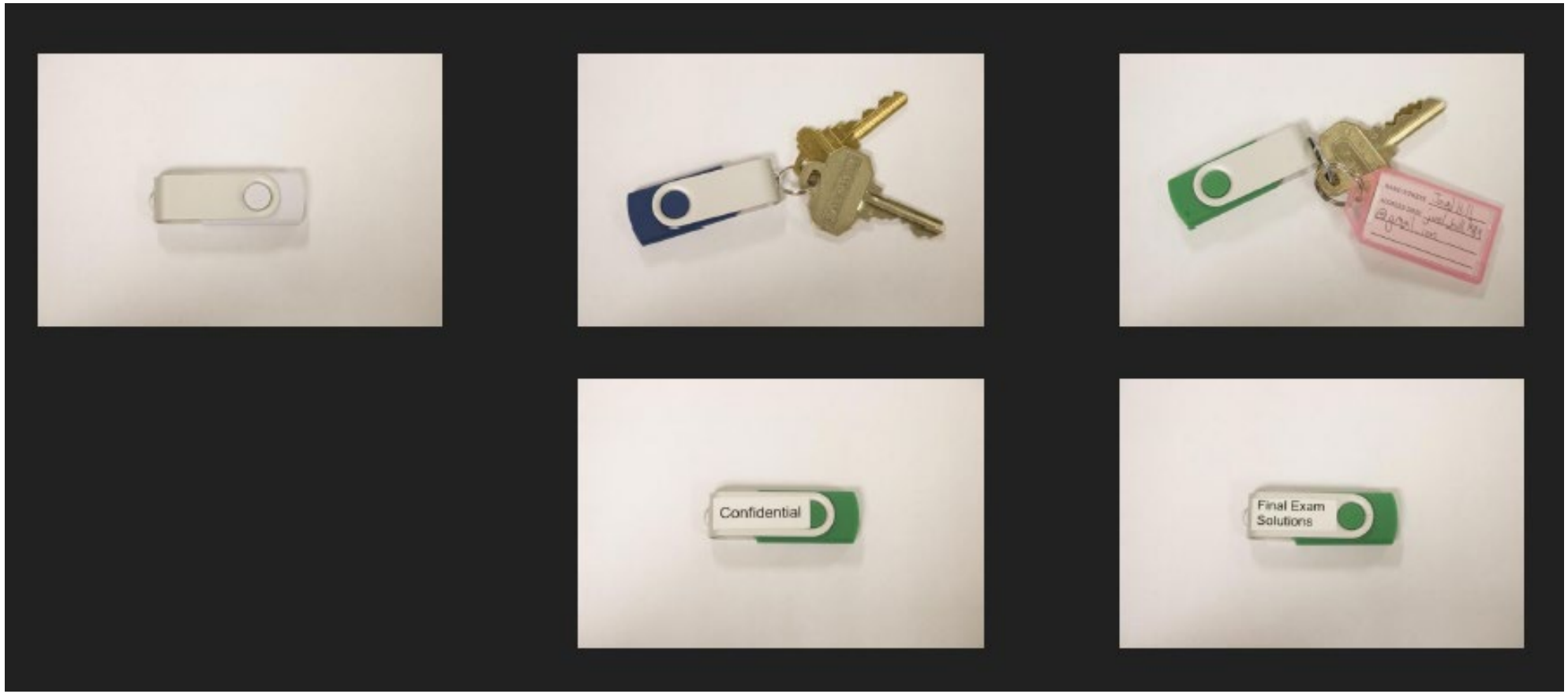
USB dropping attacks

- How effective is this method?
  - –297 social-engineering USB keys dropped on the University of Illinois campus
    - Regular USB keys with plain HTML files
    - Built a USB key creation, dropping and monitoring system

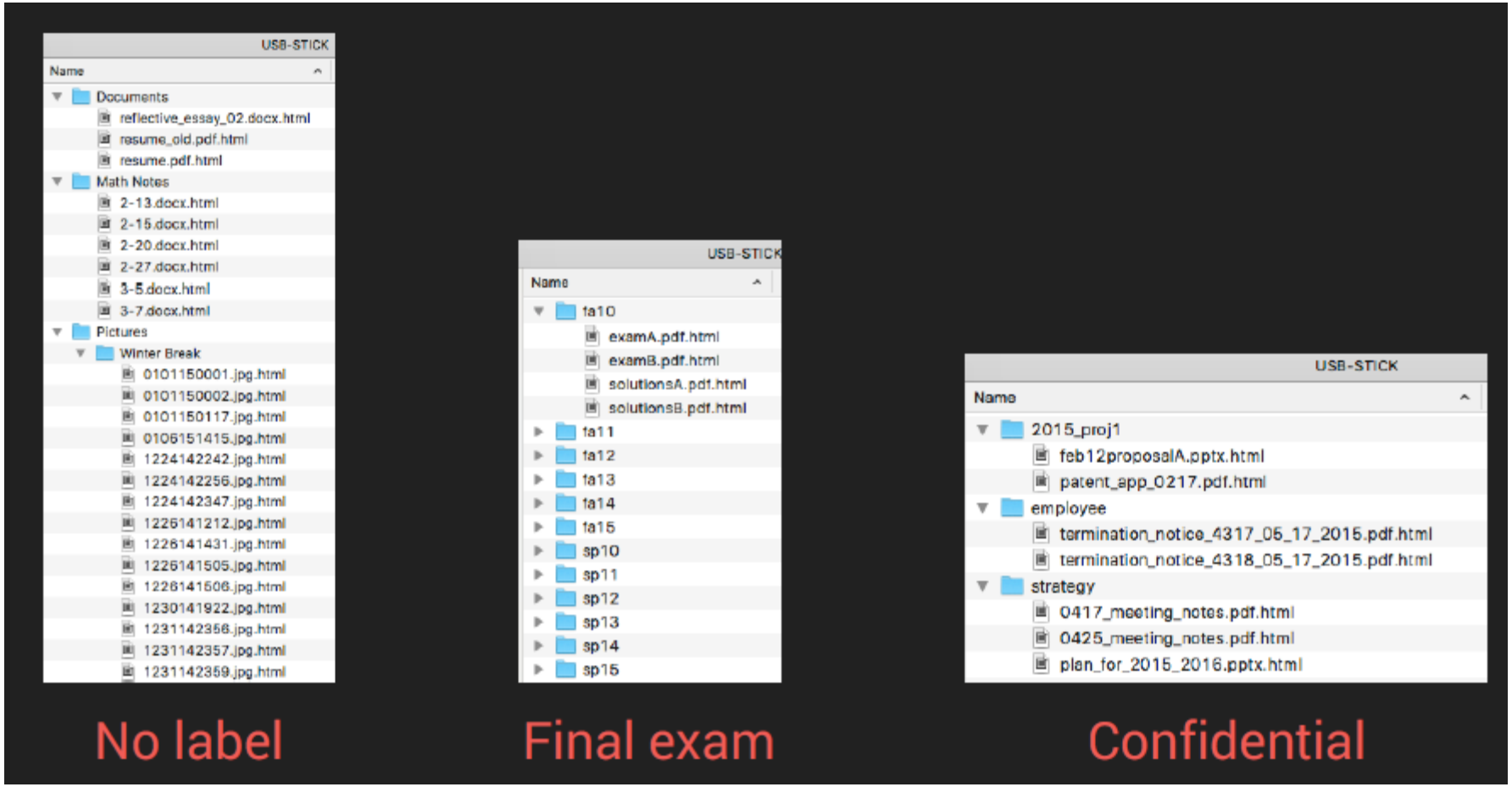
University of Illinois campus attack



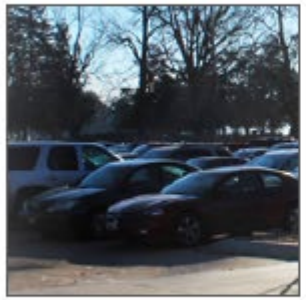
Appearance matters (?)



USB content


USB-STICK
Name
Documents
reflective_essay_02.docx.html
resume_old.pdf.html
resume.pdf.html
Math Notes
2-13.docx.html
2-15.docx.html
2-20.docx.html
2-27.docx.html
3-5.docx.html
3-7.docx.html
Pictures
Winter Break
0101150001.jpg.html
0101150002.jpg.html
0101150117.jpg.html
0106151415.jpg.html
1224142242.jpg.html
1224142256.jpg.html
1224142347.jpg.html
1226141212.jpg.html
1226141431.jpg.html
1226141505.jpg.html
1226141606.jpg.html
1230141922.jpg.html
1231142356.jpg.html
1231142357.jpg.html
1231142359.jpg.html
No label
USB-STICK
Name
fa10
examA.pdf.html
examB.pdf.html
solutionsA.pdf.html
solutionsB.pdf.html
fa11
fa12
fa13
fa14
fa15
sp10
sp11
sp12
sp13
sp14
sp15
Final exam
USB-STICK
Name
2015_proj1
feb12proposalA.pptx.html
patent_app_0217.pdf.html
employee
termination_notice_4317_05_17_2015.pdf.html
termination_notice_4318_05_17_2015.pdf.html
strategy
0417_meeting_notes.pdf.html
0425_meeting_notes.pdf.html
plan_for_2015_2016.pptx.html
Confidential

Campus location types



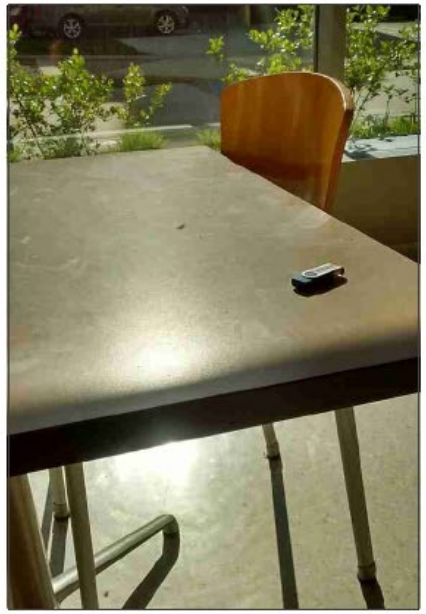
Parking lot

Outside

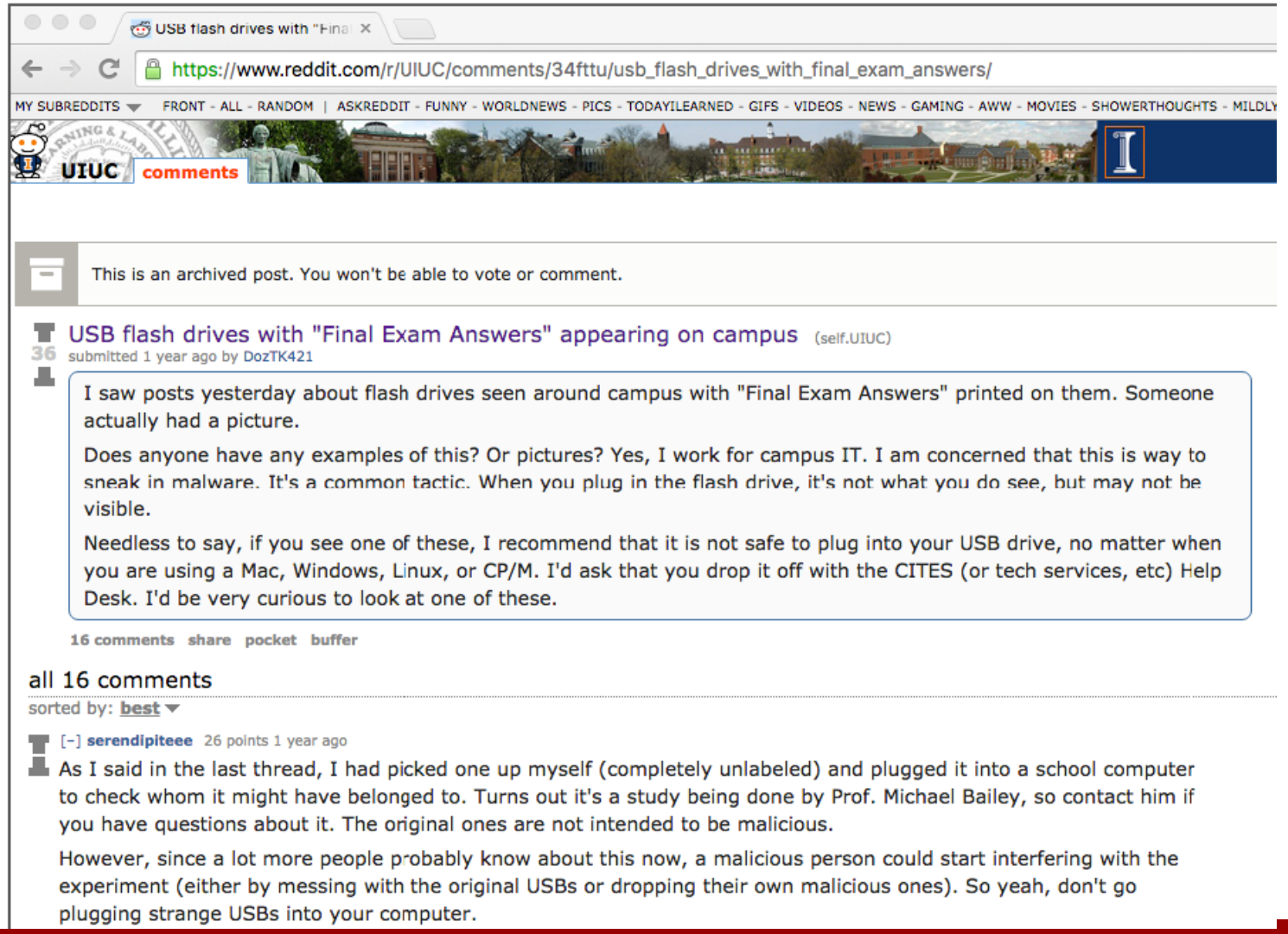
Common room

Classroom

Hallway



(Reddit busted)

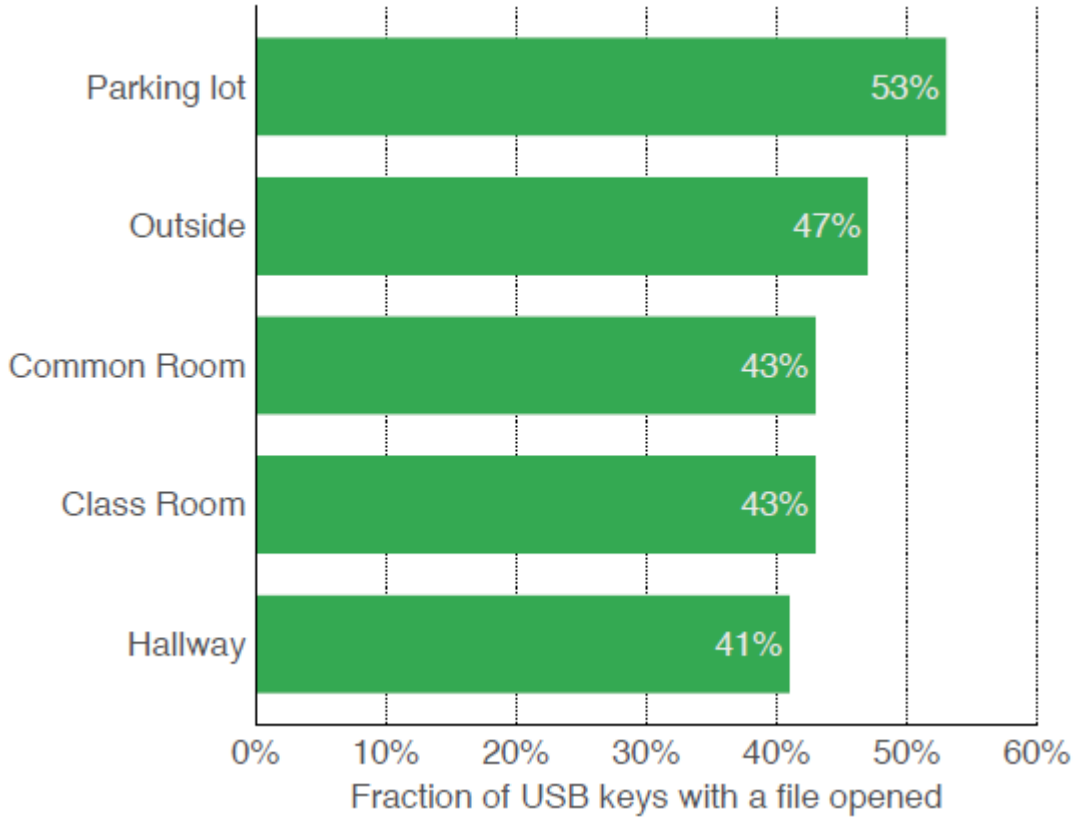


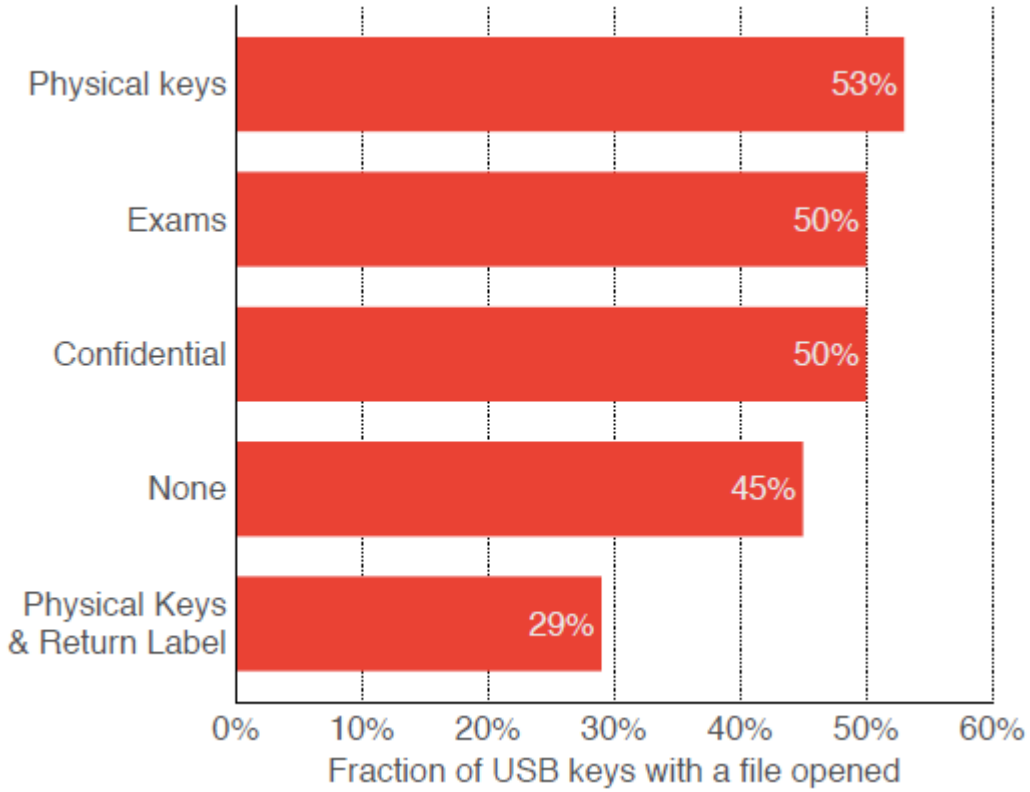
Results

- How many USBs do you think phoned home?

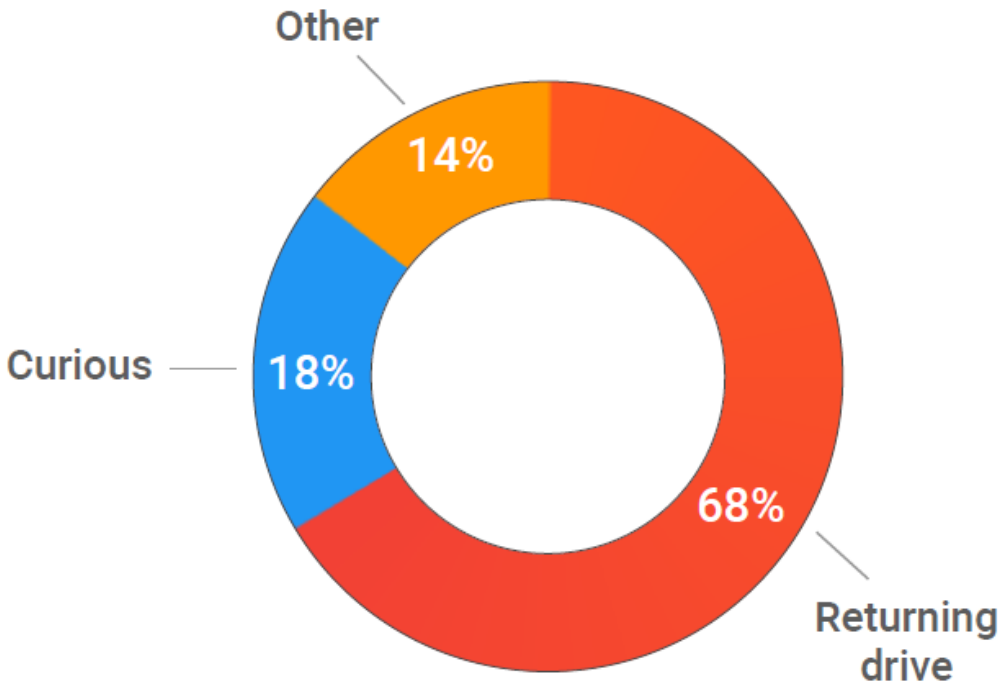
	Total	Fraction
Key dropped	297	
Key picked up	290	98%
Key who phoned home	135	45%
Key returned	54	19%
People answering survey	62	21%

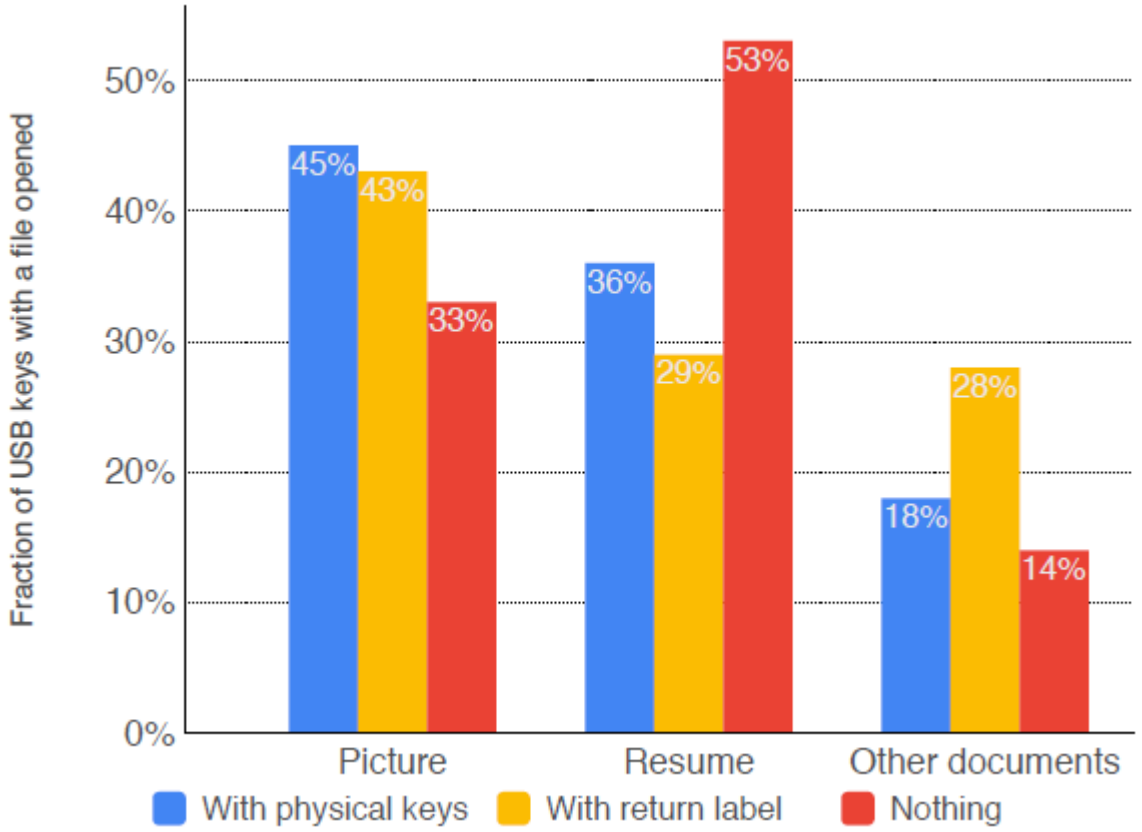
Location & appearance





Survey


Other
14%
Curious
18%
68%
Returning drive


Fraction of USB keys with a file opened
50%
40%
30%
20%
10%
0%
45%
43%
33%
36%
29%
53%
18%
28%
14%
Picture
Resume
Other documents
With physical keys
With return label
Nothing

DTU USB/QR CODE EXPERIMENTS

part of the MSc thesis of Johannes Nordskov Pedersen

QR code poster attacks

- **80 posters** in total, scattered all around the DTU campus
  - 40 offering a 150dkk coupon for the canteens
  - 40 offering 5000dkk

- Many went down since we did not follow the DTU poster rules

- **Results**
  - Total QR scans **734**
    - **413** food posters
    - **321** 5000dkk posters

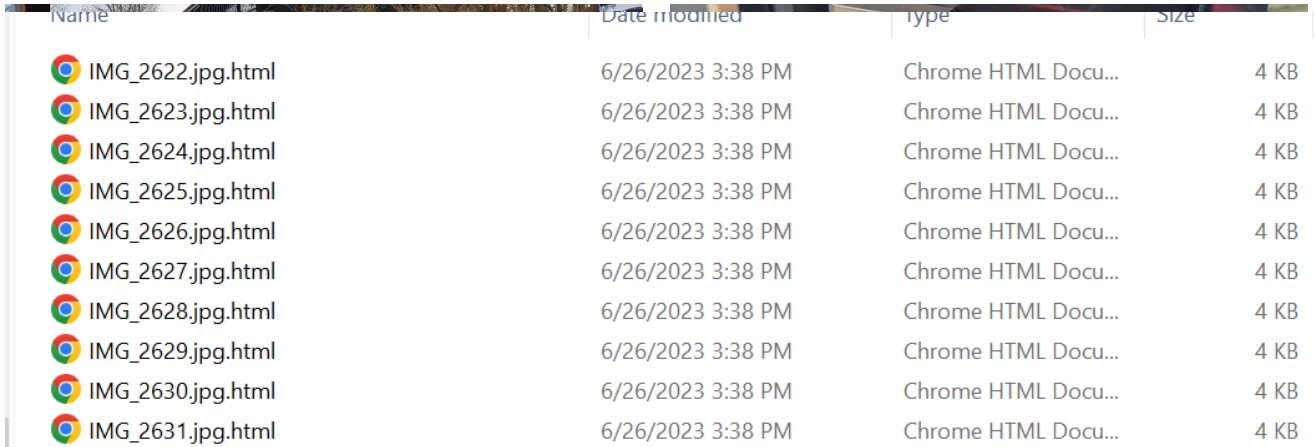
USB experiment timeline

- We requested approval in terms of legal/ethical/etc. concerns from our department in **December 2023**
- The experiment started in **March 2024** morning by placing **143 USB sticks** all around the DTU campus
  - USBs contain **no malicious files**; only a ping to our own server (hosted at DTU)
  - The ping was activated by running honeytoken-like files (word and excel) as well as fake jpg files (html files with a name indicating a photo)
- We received a **complaint from DTU's central IT** on Tuesday morning
  - (while annoying this shows good response from DTU)
  - We had to stop the experiment (take down our server, so no further measurements) by Wednesday due to complaints from higher management
- Experiment effectively ran only for one day
  - Still got some interesting results

USB drop attacks attacks

- **143 USBs** in total, scattered all around the DTU campus
  - 71 single USBs
  - 72 with keys (some with 1 key and some with 2 keys)
- Placed inside/outside, in a single day
- **Results**
  - **73 files activated**
    - **xlsx**: 12, **docx**: 39, .**jpg**: 22
  - Total unique USBs activated **16**
    - **2 single, 14 with keys**
    - **9 outside, 7 inside**

Name	Date modified	Type
Important Documents	10/10/2023 4:38 PM	File folder
Summer 2023	11/4/2023 12:23 PM	File folder



Name	Date modified	Type	Size
IMG_2622.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2623.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2624.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2625.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2626.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2627.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2628.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2629.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2630.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB
IMG_2631.jpg.html	6/26/2023 3:38 PM	Chrome HTML Docu...	4 KB

Name	Date modified	Type
Appraisal-preparation.docx	7/5/2023 5:34 AM	Microsoft Word Doc...
Budget.xlsx	5/13/2023 12:07 PM	Microsoft Excel Work...
Instalment-2024.xlsx	8/2/2023 6:16 AM	Microsoft Excel Work...
Letter-of-appointment.docx	5/15/2023 2:23 AM	Microsoft Word Doc...
Meeting-notes.docx	8/11/2023 2:37 PM	Microsoft Word Doc...
Resume.docx	8/16/2023 7:59 AM	Microsoft Word Doc...
Salary-draft.docx	10/20/2023 8:50 AM	Microsoft Word Doc...

Discussion: what do you think of the results?

USB HID ATTACKS

Ruber ducky

- Programmable HID
- Looks like a normal USB (almost)
- “Ducky Script” language
- Con: OS specific

Basic scripting example

- DELAY 1000
- GUI r
- DELAY 100
- STRING c:\windows\notepad.exe
- ENTER
- DELAY 1000
- STRING Hello World

More advanced code…

credentials	Create datacopier	23 days ago
execution	misc: Remove .DS_Stores, add to git ignore	last month
exfiltration	misc: Remove .DS_Stores, add to git ignore	last month
general	misc: Remove .DS_Stores, add to git ignore	last month
incident_response	Misc: Fix structure of repository	3 months ago
mobile	misc: Remove .DS_Stores, add to git ignore	last month
phishing	Misc: Fix structure of repository	3 months ago
prank	misc: Remove .DS_Stores, add to git ignore	last month
recon/Tree_of_Knowledge	misc: Remove .DS_Stores, add to git ignore	last month
remote_access	Updated ReverseDucky 2 to version 1.2	6 days ago

Outline

- Carsten – Signal & Onion routing
- Introduction
- Social engineering attacks
- OSINT
- USB dropping and QR code attacks
- Lab exercise

The lab for today

- Imaginary scenario:
  - –You are hired by an APT group to **attack/infiltrate the cybersecurity engineering section** of DTU
  - –NO REAL attacks