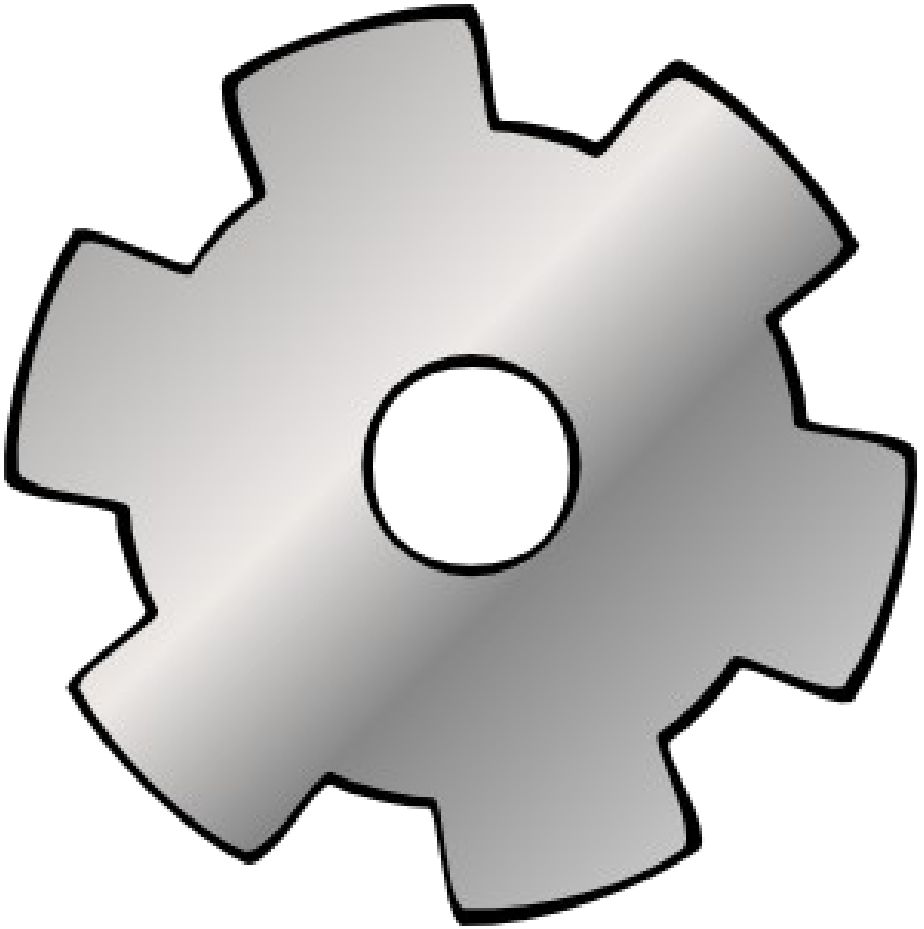
Zamyšlení nad aktuálními bezpečnostními problémy

Aleš Padrta
apadrta@cesnet.cz

CESNET, z.s.p.o.

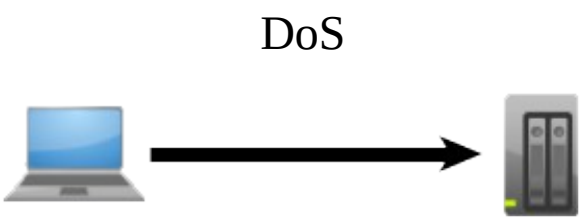
- Sdružení
  - Připojení akademických institucí
  - Další služby ...
- Bezpečnost
  - CESNET-CERTS (CSIRT)
  - Řešení incidentů
  - Co se děje v akademické síti CESNET2
  - Informace o okolí
- Pohled na aktuální bezpečnostní problémy ...

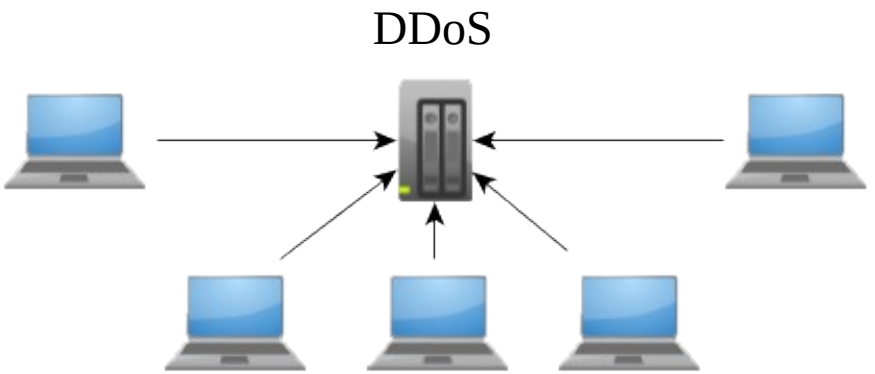
Technické problémy



Distribuovaný útok – odepření služby

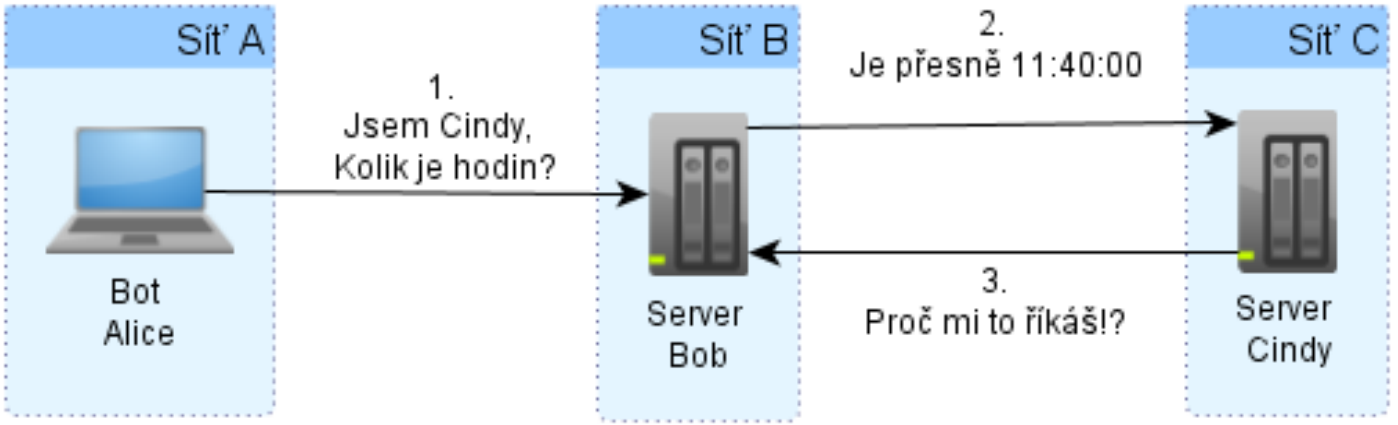
- DoS (Denial of Service)
  - Zahlcení (serveru) požadavky
    - Vyčerpání CPU, paměti, socketů, síťového pásma, ...
  - Nestíhá odpovídat regulérním uživatelům
    - Nedostupnost služby
- DDoS (Distributed DoS)
  - Více zdrojů (nelze snadno zablokovat)
    - Typicky členové botnetu





Distribuovaný útok – odepření služby

- DRDoS (Distributed Reflected Denial of Service)



- Jak je to možné?
  - Chyba v síti A:
    - Síť nechá odejít paket se zdrojem v síti C
  - Chyba v síti B:
    - Na zařízeních provozuje nepotřebné služby
    - Na serverech neomezuje přístup ke službám

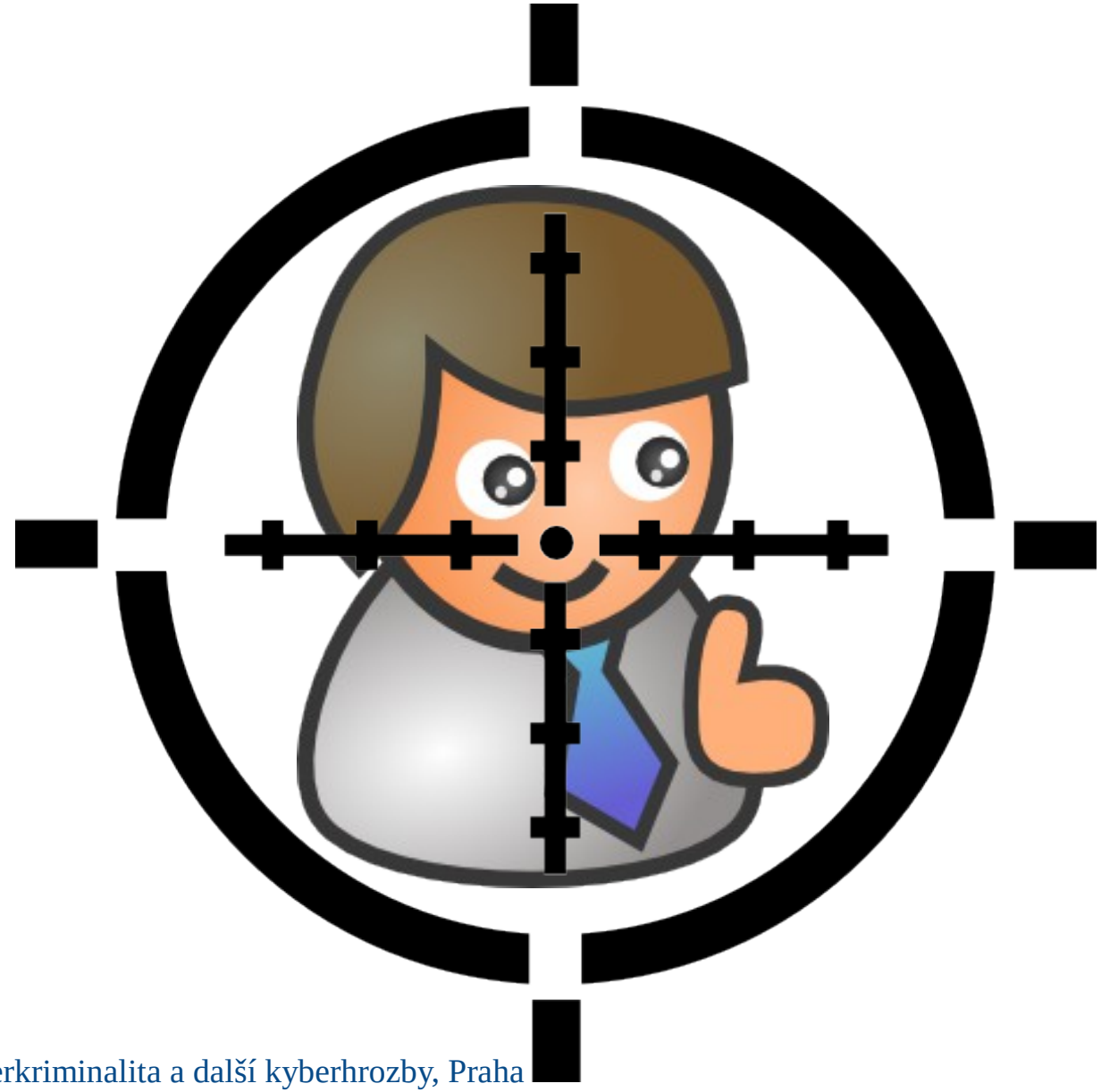
HeartBleed

- Chyba v OpenSSL
  - Přítomna řadu měsíců
  - 2/3 webových serverů
- Princip
  - Klient: Jestli jsi tam, zopakuj “test”, je to slovo o délce 500 znaků
  - Server: Jasný, posílám zpátky to tvoje slovo o délce 500 znaků (“test.další.obsah..heslo.je.veslo.....”)
- Následky
  - Výpis paměti … s hesly, klíči, ...

Bash ShellShock

- Chyba v shellu
  - Od verze 1.0.3
  - Září 1989 (!)
- Funkce v proměnné prostředí
  - `env x='() { :; }; echo "smula, Pustiku"'`
  - Chyba v parsování v subshellu (předání proměnných)
- Zneužití
  - Přímo v shellu
  - CGI
  - DHCP

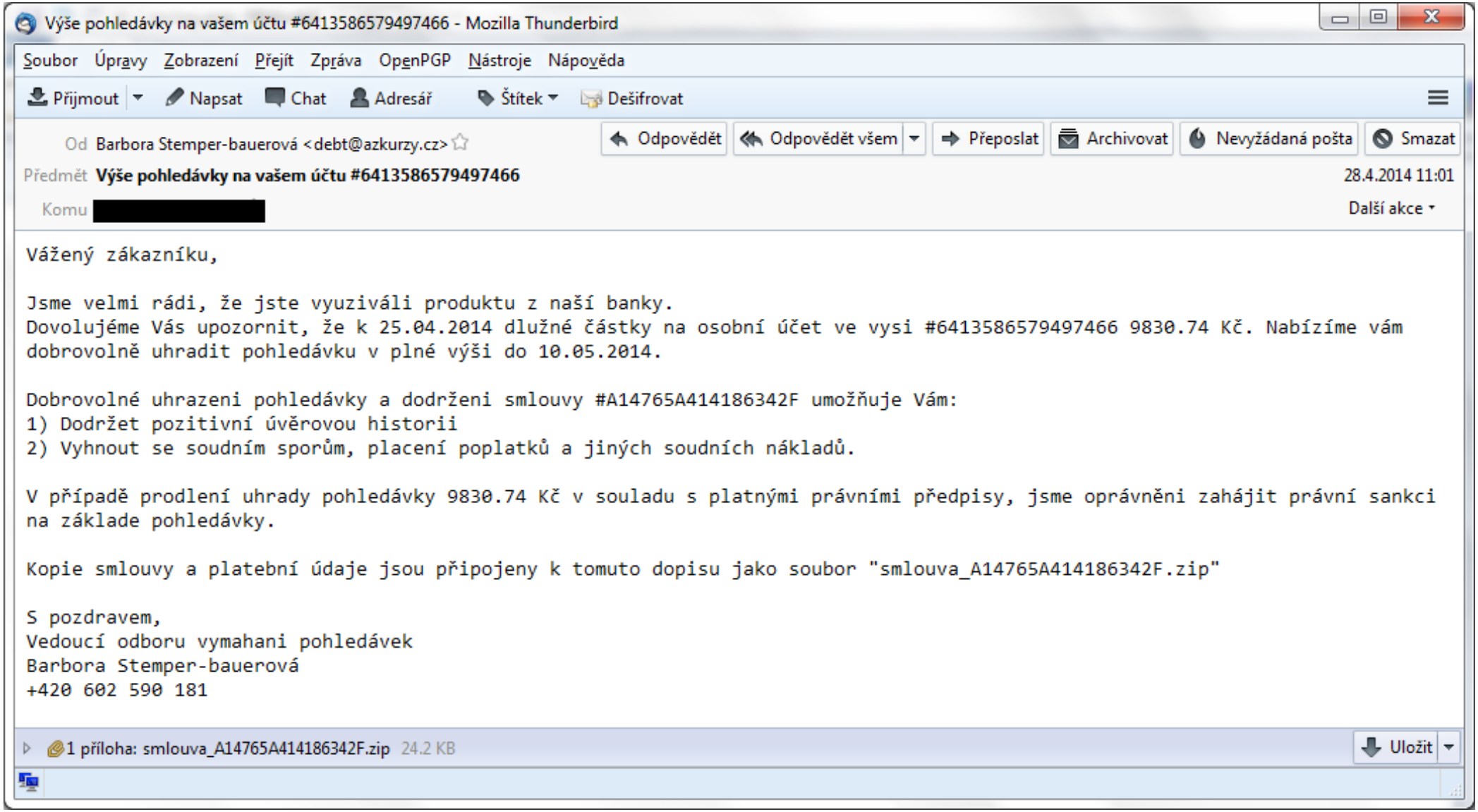
Zaměřeno na uživatele



Sociální inženýrství

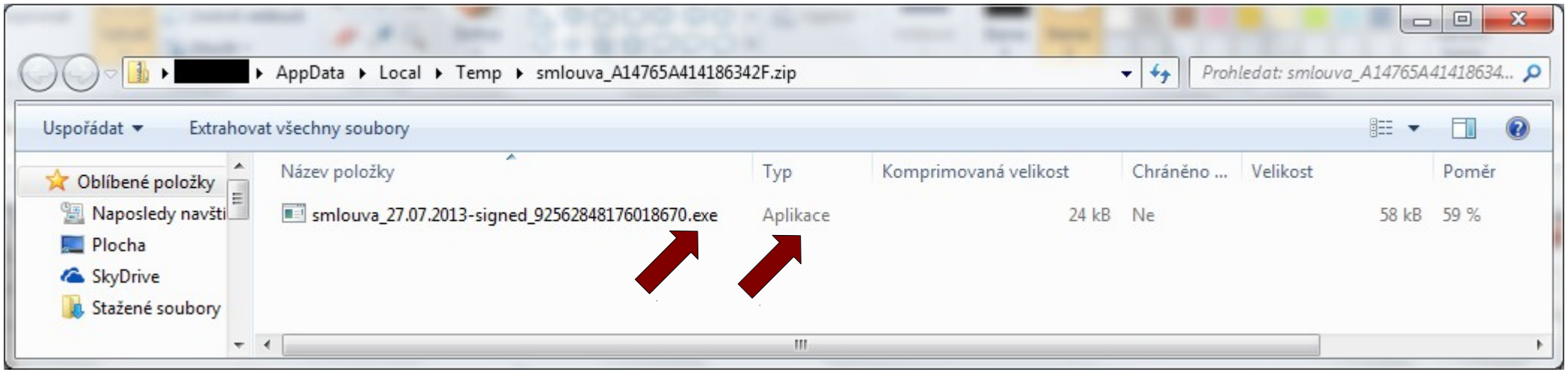
- Sociální inženýrství
  - Způsob manipulace s lidmi
  - Osvědčené psychologické postupy
- Typické znaky
  - Hrozí ztráta (i ztráta příležitosti)
  - Strašně spěchá
  - Zmínka o vyšší moci (nadřízený, soudy, …)
  - Nikdy jiný o tom nemá vědět
- Lákavé pro e-lumpy
  - Hledání zranitelnosti vs. jen přimět spustit malware

Sociální inženýrství v e-mailu



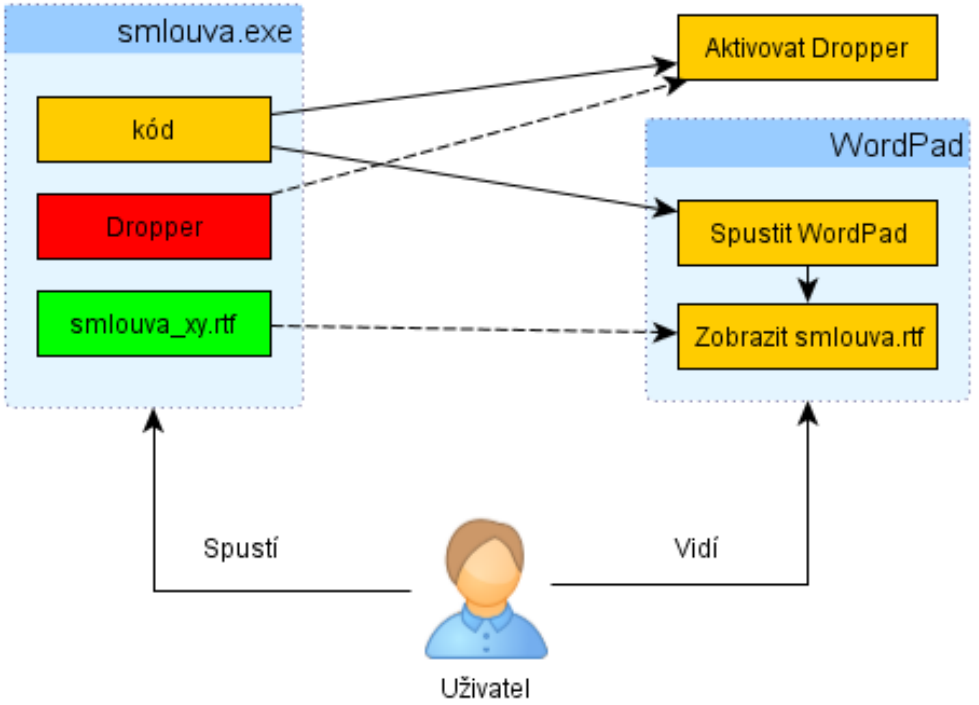
Sociální inženýrství v e-mailu

- Jasné známky SI
  - Hrozba dluhem (ztráta)
  - Zmínka o soudu (autorita)
  - Mezní datum splatnosti (stres)
- Co udělá běžný uživatel?
  - Podívá se **co a komu vlastně dluží** – do přílohy



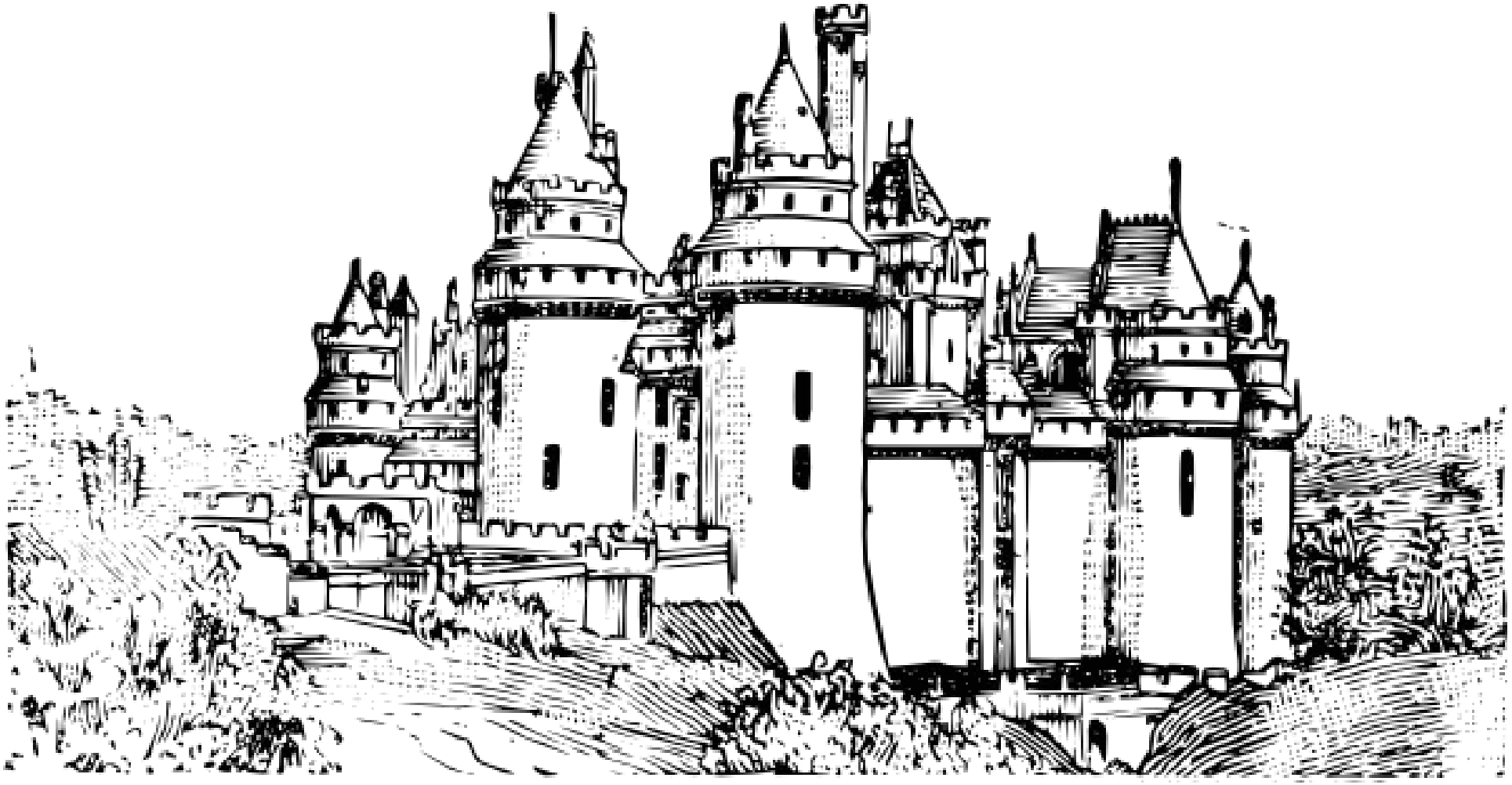
Analýza přílohy

- Analýza FLAB CESNET



- Instalovaný malware
  - Týden od 28.4.2014 … testovací botnet klient
  - Týden od 5.5.2014 … zapojení do botnetu ZEUS

Jak zvýšit svou bezpečnost?



Jak zvýšit svou bezpečnost?

- Stále stejné … už staří římané ...
  - Scientia est potentia (ve vědění je síla)
- Jak se připravit?
  - Základní technické prostředky
    - Správné, Správně nastavené, Udržované
  - Mít informace o aktuálních problémech
    - Vzdělávat se, být ve střehu
- Není v moci běžných uživatelů
- Kdo může pomoci?
  - **Bezpečnostní týmy jsou tu pro vás**

Dotazy

???