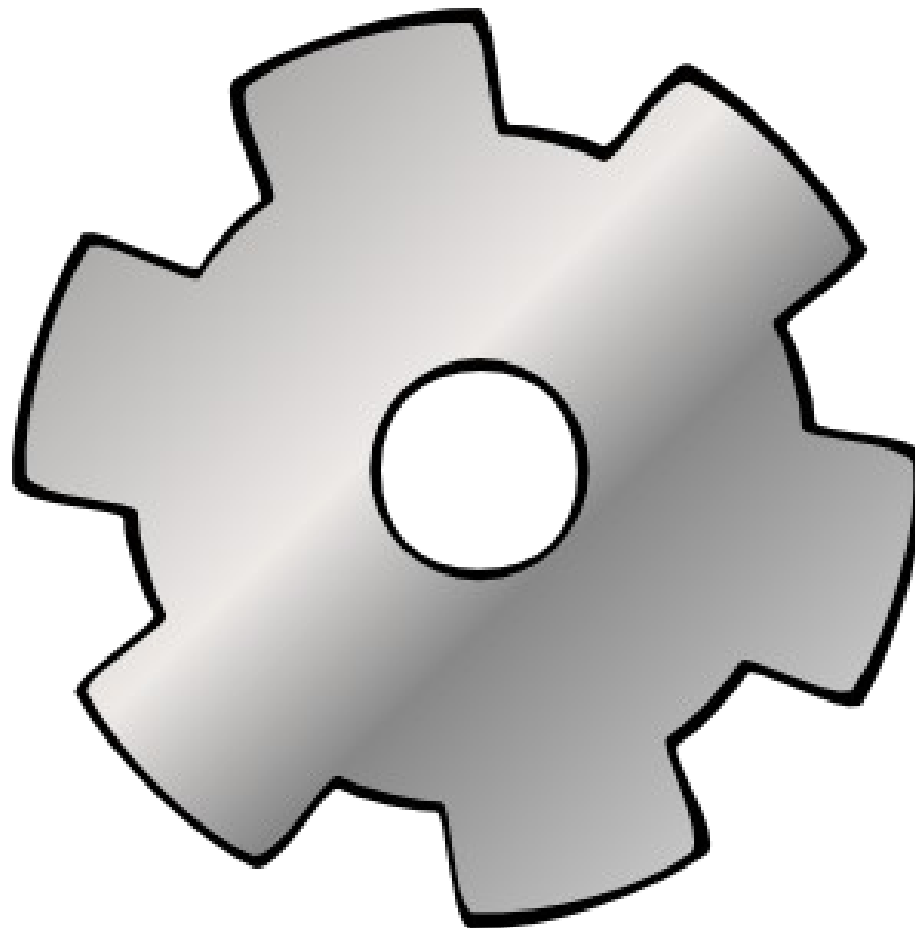


# Zamyšlení nad aktuálními bezpečnostními problémy

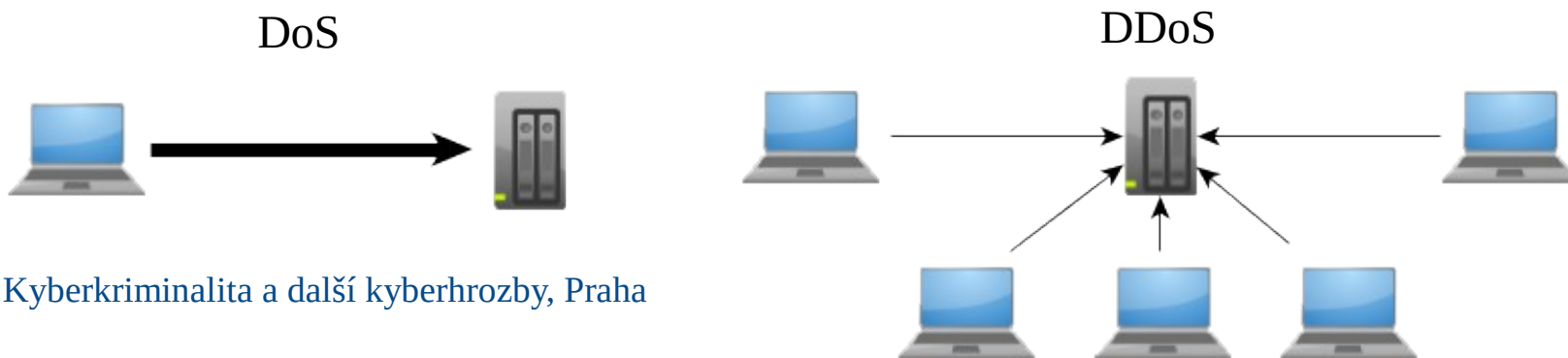
Aleš Padrta  
[apadrta@cesnet.cz](mailto:apadrta@cesnet.cz)

- 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 ...

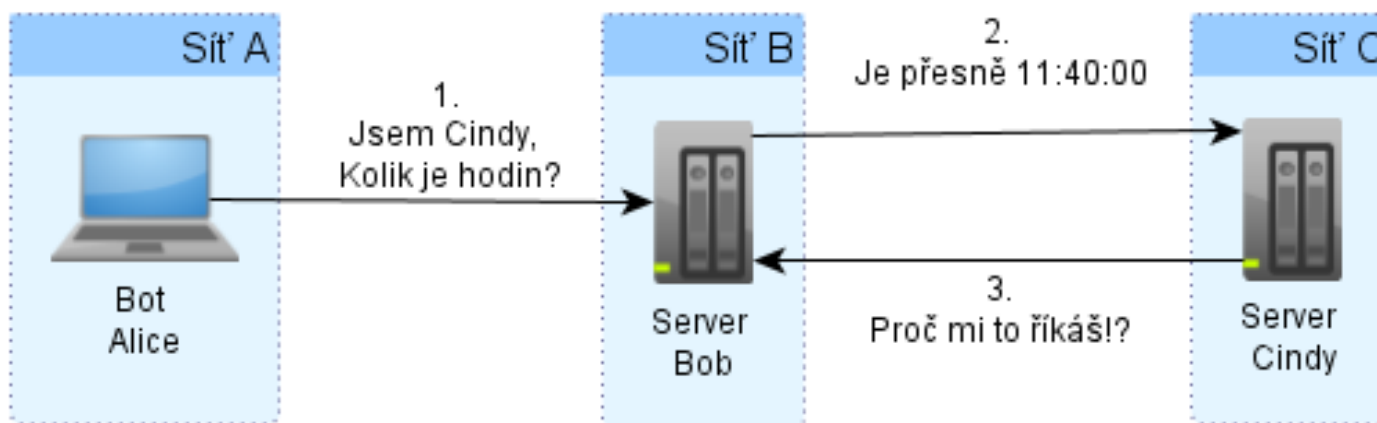
# Technické problémy



- 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



- 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

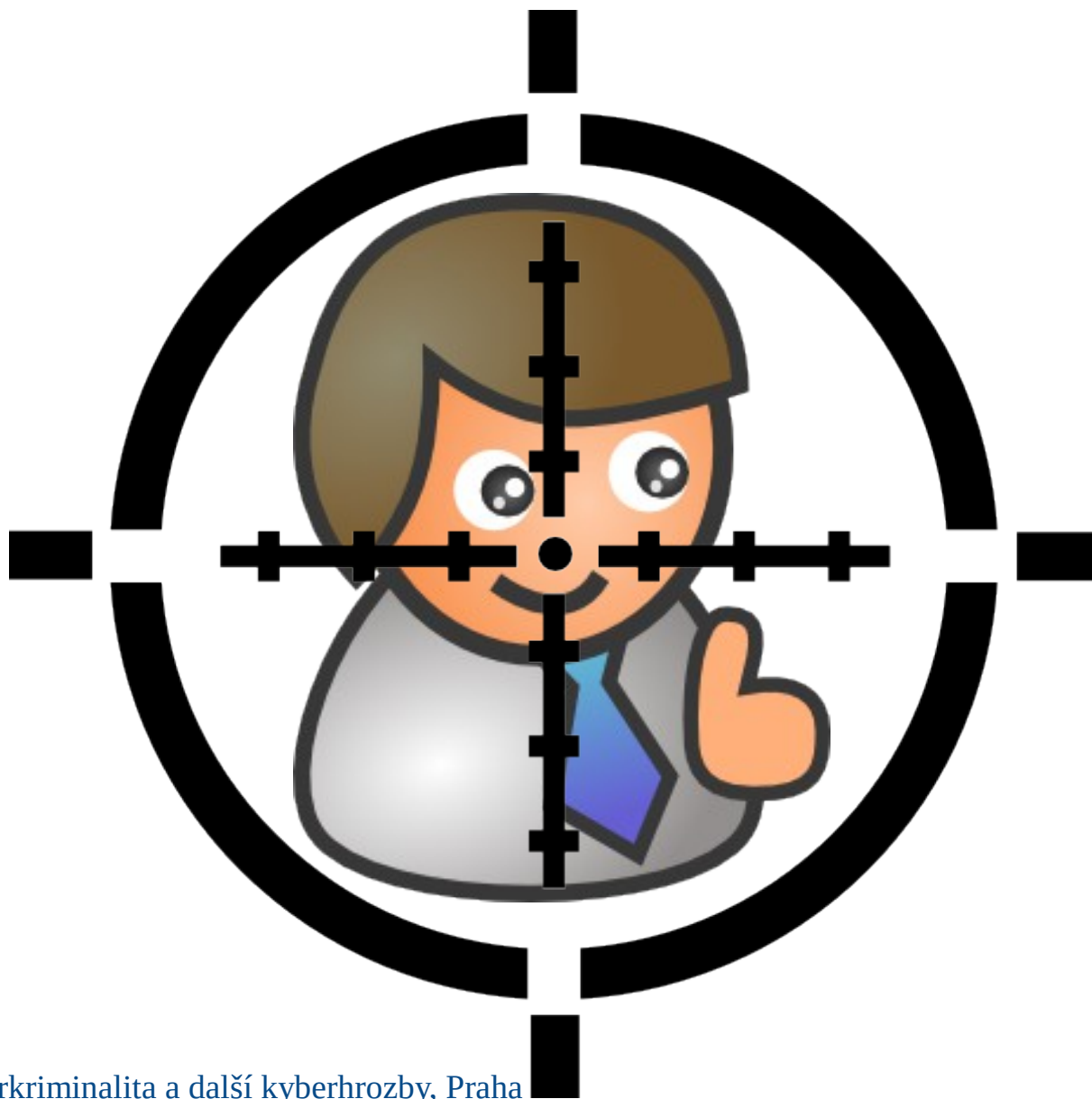
- Chyba v OpenSSL
  - Přítomna řadu měsíců
  - 2/3 webových serverů
- Princip
  - Klient: Jestli jsi tam, zopakuj “test”, je to slovo o délce 500 znaků
  - Server: Jasný, posílám zpátky to tvoje slovo o délce 500 znaků (“test.další.obsah..heslo.je.veslo.....”)
- Následky
  - Výpis paměti ... s hesly,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



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

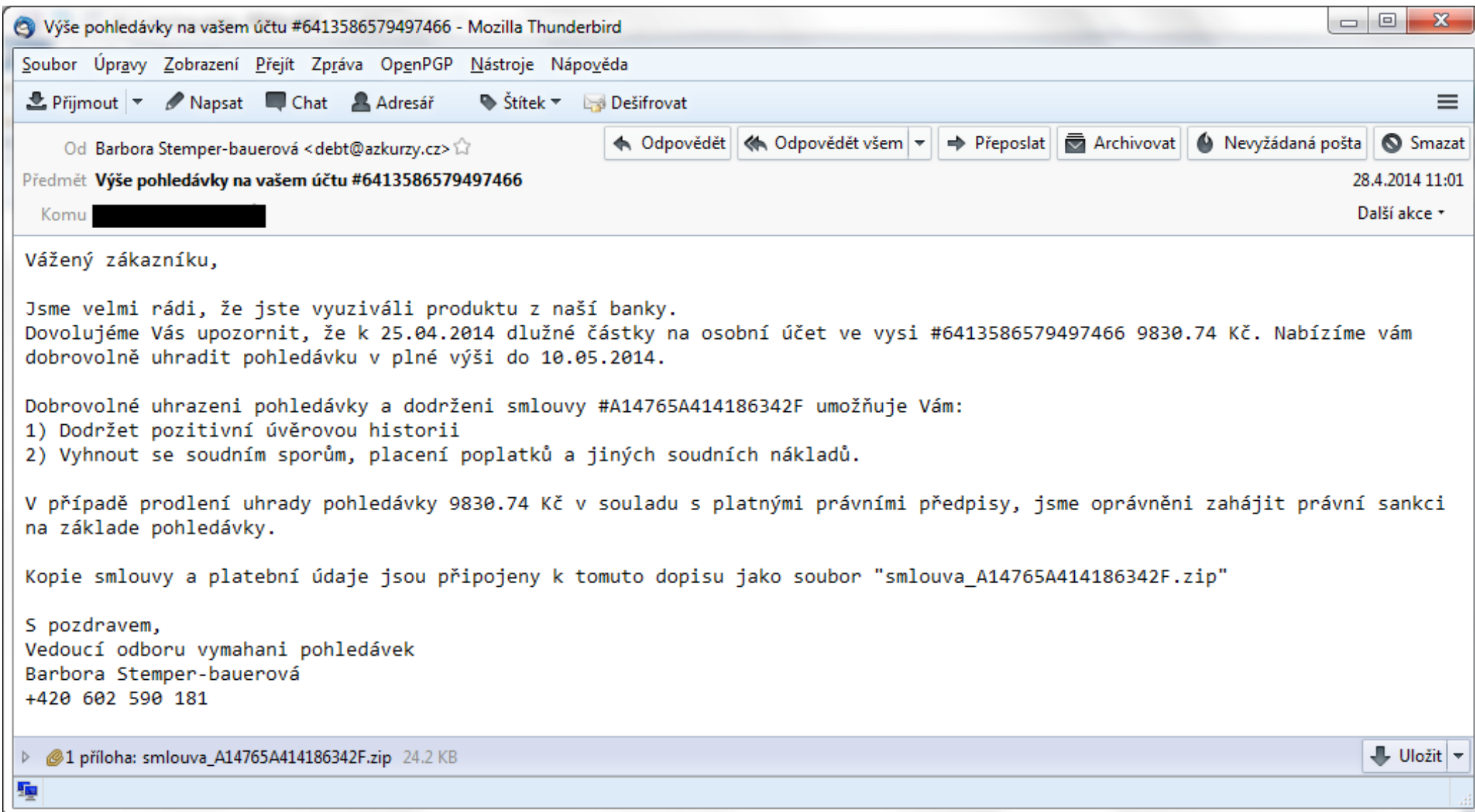


# Zaměřeno na uživatele





- Sociální inženýrství
  - 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



Výše pohledávky na vašem účtu #6413586579497466 - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva OpenPGP Nástroje Nápořádá

Přijmout Napsat Chat Adresář Štítek Dešifrovat

Od Barbora Stemper-bauerová <debt@azkurzy.cz> ☆

Odpovědět Odpovědět všem Přeposlat Archivovat Nevyžádaná pošta Smazat

Předmět **Výše pohledávky na vašem účtu #6413586579497466** 28.4.2014 11:01

Komu [redacted] Další akce ▾

Vážený zákazníku,

Jsme velmi rádi, že jste vyuzivali produktu z naší banky. Dovolujeme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysí #6413586579497466 9830.74 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 10.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #A14765A414186342F umožňuje Vám:

- 1) Dodržet pozitivní úvěrovou historii
- 2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

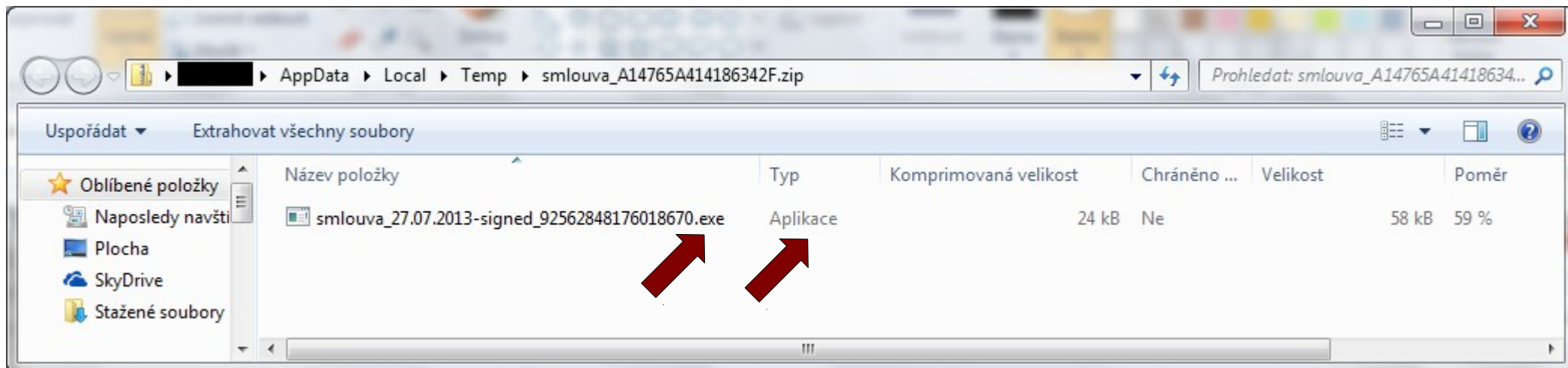
V případě prodlení uhrady pohledávky 9830.74 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základe pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva\_A14765A414186342F.zip"

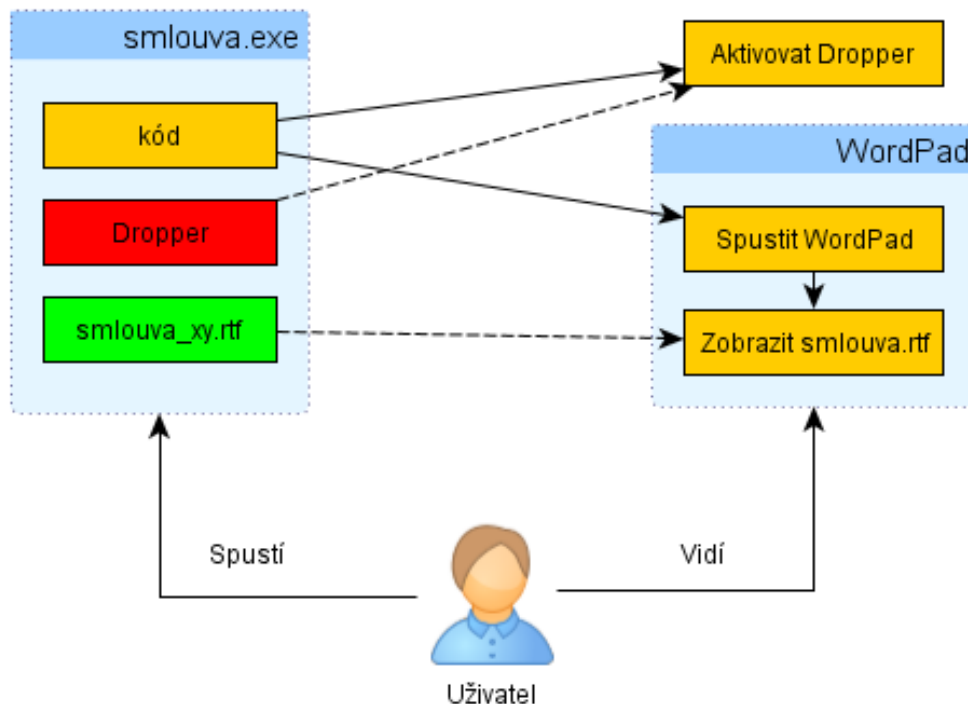
S pozdravem,  
Vedoucí odboru vymahání pohledávek  
Barbora Stemper-bauerová  
+420 602 590 181

1 příloha: smlouva\_A14765A414186342F.zip 24.2 KB Uložit ▾

- Jasně 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



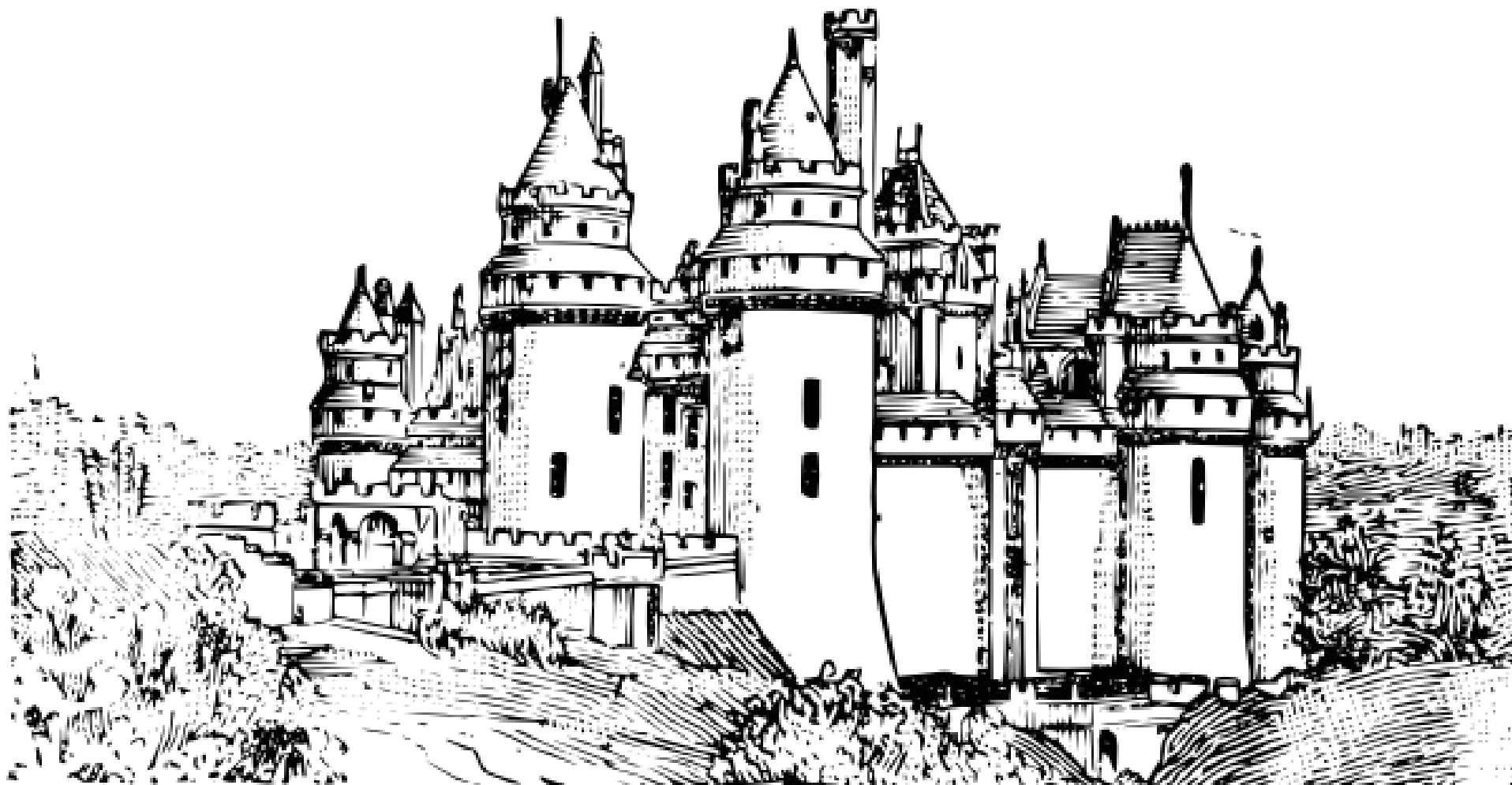
- Analýza FLAB CESNET



- 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

???