POLICIE ČESKÉ REPUBLIKY

KRAJSKÉ ŘEDITELSTVÍ ÚSTECKÉHO KRAJE
ODBOR HOSPODÁŘSKÉ KRIMINALIY

Podvodné
e-mailové zprávy

Úvod do problematiky

- Podvodné e-mailové zprávy začaly být ve větším měřítku šířeny od dubna roku 2014,
- Jedná se o elektronickou komunikaci, kde koncový zákazník je vyzván k rozbalení přílohy, buď ve formátu „zip“, nebo „exe“,
- Příloha skrývá tzv. trojského koně, tedy program, který se sám instaluje do počítače, kde je neaktivní do doby, než je aktivován útočníkem.

Existují tři druhy oznámení

1. Občanem, který obdržel podvodný e-mail s výzvou k úhradě nějaké částky,
   - ✓ Není uveden věřitel,
   - ✓ Číslo účtu je fiktivní,
   - ✓ Jméno a příjmení pracovníka je smýšlené
   - ✓ Telefonní kontakt je náhodný,

   Cílem útočníka je, aby adresát otevřel zazipovaný soubor, a tak infikoval svůj počítač.

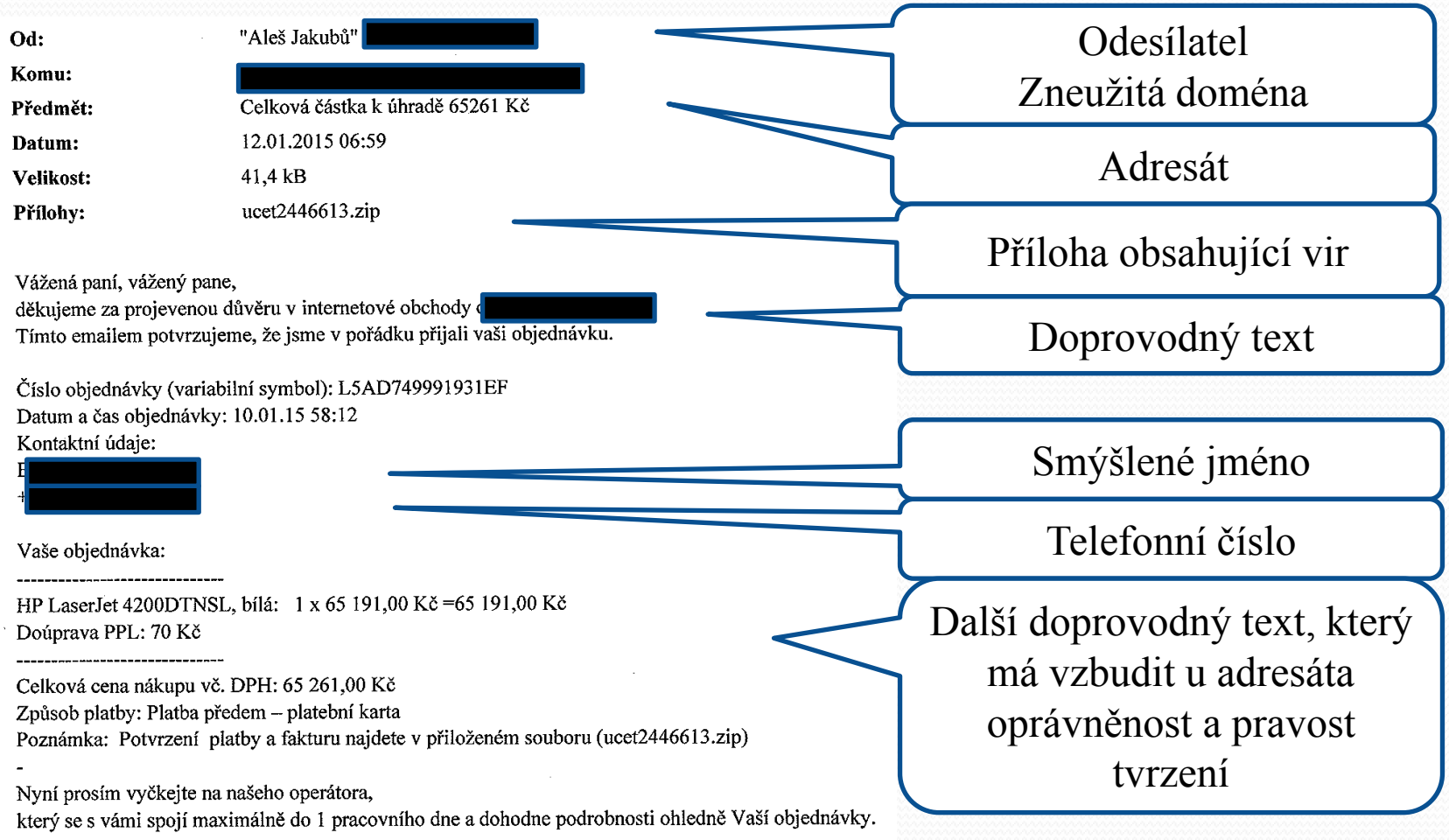
Existují tři druhy oznámení

2. Občanem, který vlastní uvedené telefonní číslo v doprovodném textu,
   - ✓ Této osobě je voláno i cca 40x denně,
   - ✓ Jedná se o nepříjemné a obtěžující hovory,
3. Společností, u které došlo ke zneužití jejich obchodní domény,
   - ✓ Mezi společnostmi jsou i drobní živnostníci, školy, ale i státní instituce,

Čtyři druhy podvodných e-mailů

1) Počátkem roku 2014 – smýšlené zprávy pod hlavičkou jedné státní organizace, /celkem 4 vlny/
2) V dubnu 2014 smyšlené zprávy pod hlavičkou neexistující banky /celkem 6 vln/
3) V červenci smýšlené zprávy pod hlavičkou existujících exekutorů /celkem 7 vln/
   - V této době rovněž smýšlené zprávy od bankovního ústavu, /celkem 10 vln/
4) V současné době smýšlené zprávy od internetového prodejce, /evidujeme cca 50 oznámení/

Ukázka podvodných e-mailových zpráv



Od: "Aleš Jakubů" [redacted]
Komu: [redacted]
Předmět: Celková částka k úhradě 65261 Kč
Datum: 12.01.2015 06:59
Velikost: 41,4 kB
Přílohy: ucet2446613.zip

Vážená paní, vážený pane,
děkujeme za projevenou důvěru v internetové obchody [redacted]
Tímto emailem potvrzujeme, že jsme v pořádku přijali vaši objednávku.

Číslo objednávky (variabilní symbol): L5AD749991931EF
Datum a čas objednávky: 10.01.15 58:12
Kontaktní údaje:
[redacted]
[redacted]

Vaše objednávka:

HP LaserJet 4200DTNSL, bílá: 1 x 65 191,00 Kč =65 191,00 Kč
Doúprava PPL: 70 Kč

Celková cena nákupu vč. DPH: 65 261,00 Kč
Způsob platby: Platba předem – platební karta
Poznámka: Potvrzení platby a fakturu najdete v přiloženém souboru (ucet2446613.zip)
-
Nyní prosím vyčkejte na našeho operátora,
který se s vámi spojí maximálně do 1 pracovního dne a dohodne podrobnosti ohledně Vaší objednávky.

Odesílatel
Zneužitá doména

Adresát

Příloha obsahující vir

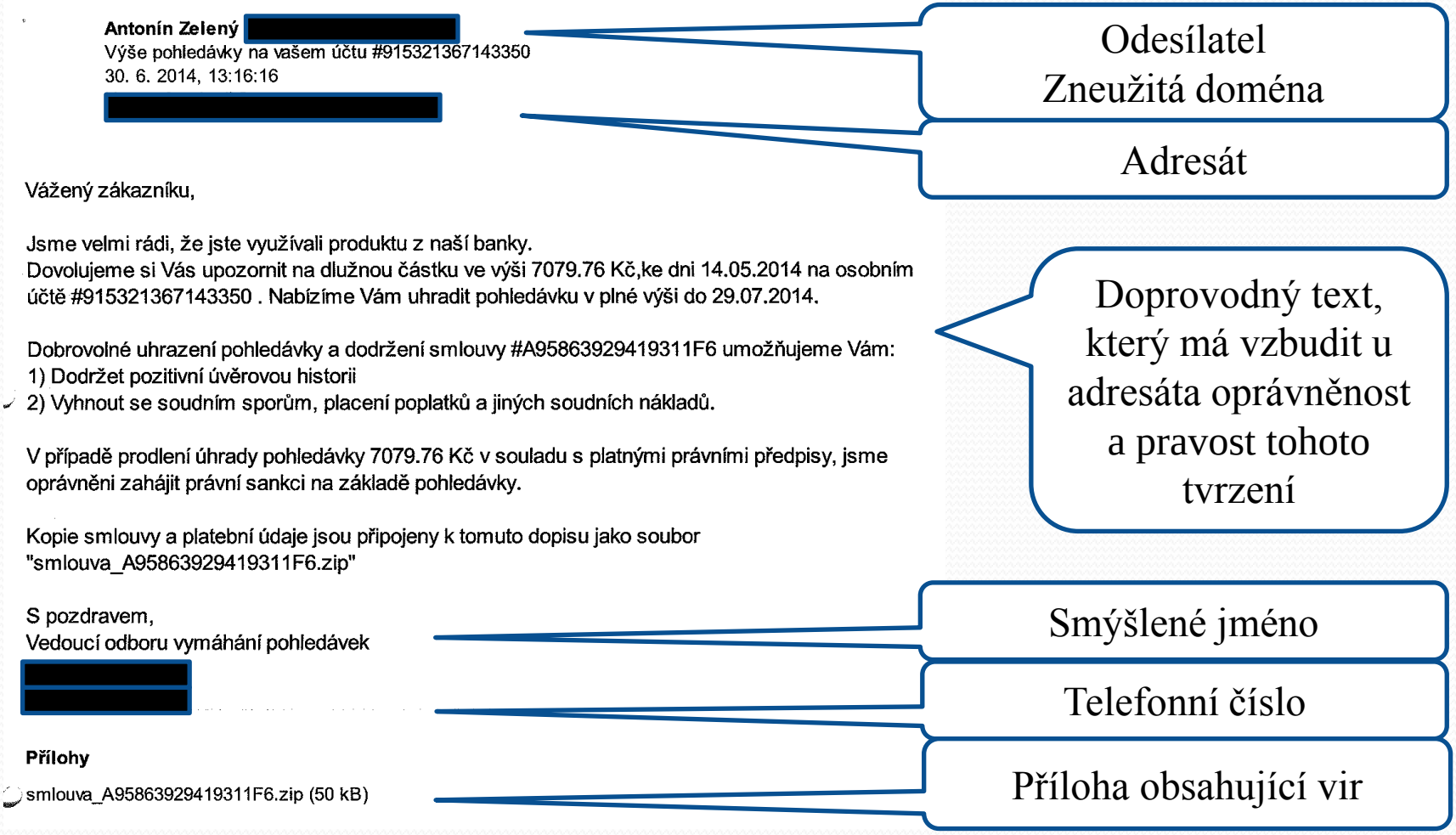
Doprovodný text

Smýšlené jméno

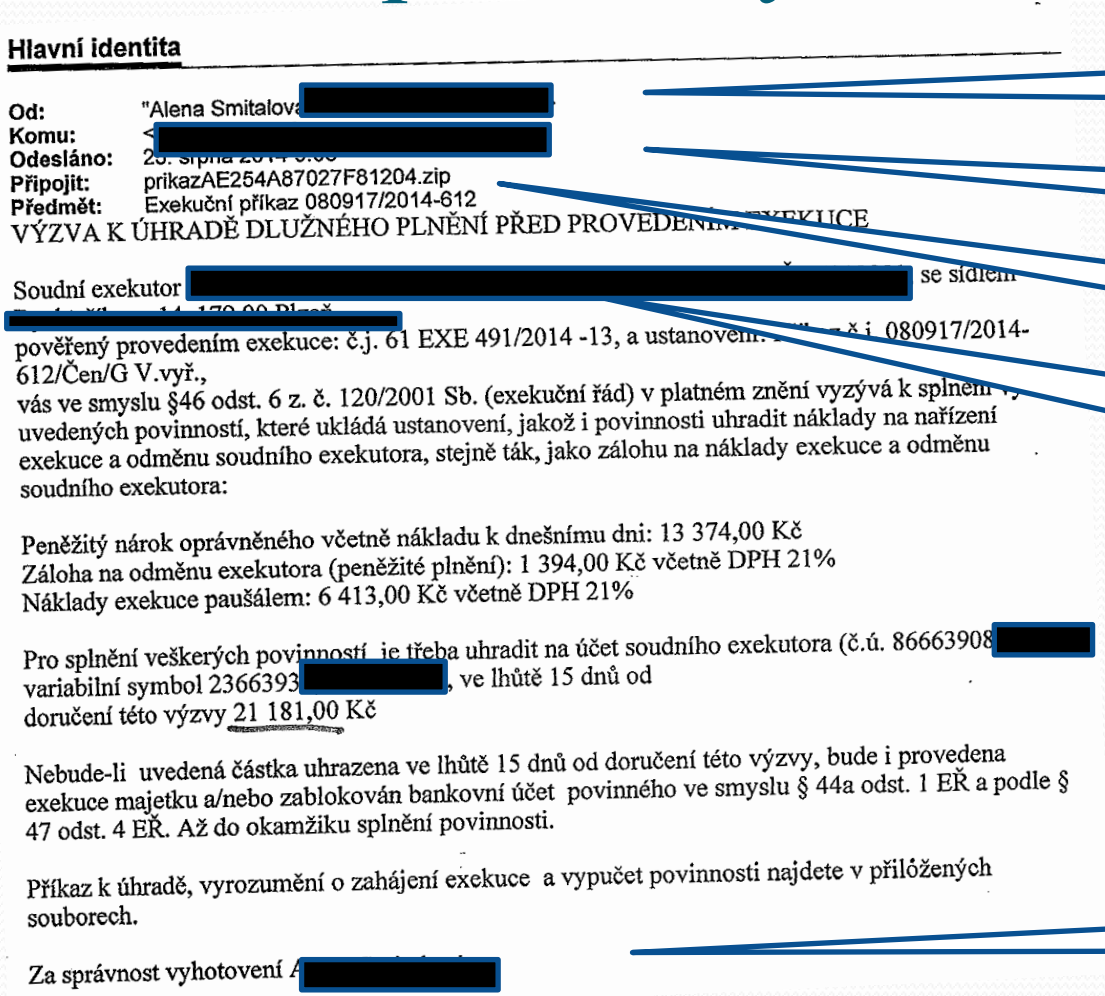
Telefonní číslo

Další doprovodný text, který má vzbudit u adresáta oprávněnost a pravost tvrzení

Ukázka podvodných e-mailových zpráv



Ukázka podvodných e-mailových zpráv



Hlavní identita

Od: "Alena Smitalova [redacted]
Komu: [redacted]
Odesláno: 25. srpna 2014 9:08
Připojit: prikazAE254A87027F81204.zip
Předmět: Exekuční příkaz 080917/2014-612

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor [redacted] se sídlem [redacted]
pověřený provedením exekuce: č.j. 61 EXE 491/2014 -13, a ustanovením [redacted] č.j. 080917/2014-612/Čen/G V.vyř.,
vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění [redacted] uvedených povinností, které ukládá ustanovení, jakož i povinnosti uhradit náklady na nařízení exekuce a odměnu soudního exekutora, stejně tak, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 13 374,00 Kč
Záloha na odměnu exekutora (peněžité plnění): 1 394,00 Kč včetně DPH 21%
Náklady exekuce paušálem: 6 413,00 Kč včetně DPH 21%

Pro splnění veškerých povinností je třeba uhradit na účet soudního exekutora (č.ú. 86663908[redacted] variabilní symbol 2366393[redacted], ve lhůtě 15 dnů od doručení této výzvy 21 181,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku splnění povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení A[redacted]

Odesílatel

Adresát

Příloha obsahující vir

Zneužité jméno soudního exekutora

Doprovodný text, který má vzbudit u adresáta oprávněnost a pravost tohoto tvrzení

Smýšlené jméno

Ukázka podvodných e-mailových zpráv

Od: "Barbora Pavlišová" [redacted]
Komu: [redacted]
Předmět: Výše pohledávky na vašem účtu #8419755534914938
Datum: 13.05.2014 13:21
Velikost: 49,8 kB
Přílohy: smlouva_34139C49210492F6.zip

Odesílatel

Adresát

Příloha obsahující vir

Vážený zákazníku,

Jsme velmi rádi, že jste využívali produktu z naší banky.
Dovolujeme si Vás upozornit na dlužnou částku ve výši 8194.88 Kč,ke dni 15.04.2014 na osobním účtě #8419755534914938 . Nabízíme Vám uhradit pohledávku v plné výši do 29.05.2014.

Dobrovolné uhrazení pohledávky a dodržení smlouvy #34139C49210492F6 umožňujeme Vám:
1) Dodržet pozitivní úvěrovou historii
2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení úhrady pohledávky 8194.88 Kč v souladu s platnými právními předpisy, jsme oprávněni zahájit právní sankci na základě pohledávky.

Kopie smlouvy a platební údaje jsou připojeny k tomuto dopisu jako soubor "smlouva_34139C49210492F6.zip"

Doprovodný text, který má vzbudit u adresáta oprávněnost a pravost tohoto tvrzení

S pozdravem,
Vedoucí odboru vymáhání pohledávek
[redacted]

Smýšlené jméno

Telefonní číslo

Rozsah útoků

- Policie ČR v současné době disponuje dostatkem informací a materiálů,
- Policie ČR již neprovádí zajišťování materiálů u oznamovatelů,
- Policie ČR KŘP Ústeckého kraje zpracovává a vyhodnocuje cca 3000 oznámení z celé ČR
- Policie ČR pomocí specializovaných pracovišť provádí zjišťování a získávání informací k útočníkovi,

Způsobená škoda

- Neoprávněně napadená počítačová jednotka
  - Nebezpečnost spočívá ve využití:
    1. Získání informací k internetovému bankovnictví,
    2. Získání osobních /pracovních/ dat,
    3. Příprava na ovládnutí počítačové jednotky k napadnutí různých institucí,
- Přečin Neoprávněný přístup k počítačovému systému a nosiči informací dle ust. § 230, odst. 2 písm. a) d) trestního zákoníku,
- Trestní sazba až 2 léta, zákaz činnosti, propadnutí věci,

Prevence – opatření

- V případě obdržení neznámého e-mailu nikdy NEOTEVÍRAT přílohy,
- Podezřelé e-mailové zprávy smazat,
- Zkontrolovat PC antivirovým programem, v současnosti již antivirové programy detekují tyto e-maily a mažou je, nebo nedovolí je otevřít,
- V případě, že došlo o otevření přílohy, je nutné PC nechat přeinstalovat odborníkem

Prevence – opatření

- Sledovat upozornění svého bankovního ústavu o nové modifikaci virů a podvodných e-mailů,
- Kontrolovat antivirové programy,
- Dodržovat bezpečnostní zásady při využívání internetového bankovnictví,

Upozornění majitelům BÚ

- Neumožňovat převody finančních prostředků přes svůj bankovní účet,
- Majitel účtu je osloven s nabídkou práce, či finanční výpomoci,
  - ✓Na účet mu jsou zaslány finanční prostředky, které má vyzvednout a následně přeposlat do zahraničí pomocí služeb internetového bankovnictví,
- Lze zvažovat možný trestní postih majitele účtu.

POLICIE ČESKÉ REPUBLIKY

KRAJSKÉ ŘEDITELSTVÍ ÚSTECKÉHO KRAJE
ODBOR HOSPODÁŘSKÉ KRIMINALIY

KRAJSKÉ ŘEDITELSTVÍ ÚSTECKÉHO KRAJE
ODBOR HOSPODÁŘSKÉ KRIMINALIY

Děkuji za pozornost

Mjr. Ing. Mgr. Radim Vojáček