Podvodníci zkoušejí na důvěřivce nový trik s tisícovými dluhy

Českým internetem se začaly na přelomu minulého a tohoto týdne šířit ve velkém nevyžádané zprávy, které se tváří jako oficiální e-maily od bankovních institucí. Podvodníci v nich straší příjemce dlužnými částkami v řádech tisíců korun. V příloze se však místo faktury ukrývá virus.

Desatero bezpečného internetu

1. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.

2. Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zdali funguje.

3. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.

4. Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.

5. Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou https, kde „s“ znamená bezpečná.

6. Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.

7. Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.

8. Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.

9. V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.

10. Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.

Dnes 12:31
(Aktualizováno: 12:40)

Podle ohlasů čtenářů Novinek se internetové adresy, ze kterých podvodníci odesílají zprávy, často mění. Objevily se mezi nimi například domény nerodia.cz nebo erika-as.cz.

Že se jedná o podvod, je patrné už na první pohled podle špatné diakritiky, která se v česky psaném e-mailu objevuje.

Text podvodného e-mailu

Vážený zákazníku,

Jsme velmi rádi, že jste vyuziváli produktu z naší banky. Dovolujéme Vás upozornit, že k 25.04.2014 dlužné částky na osobní účet ve vysi #9471254734256890 9292.12 Kč. Nabízíme vám dobrovolně uhradit pohledávku v plné výši do 13.05.2014.

Dobrovolné uhrazeni pohledávky a dodrženi smlouvy #22365A830317939E umožňuje Vám:

1) Dodržet pozitivní úvěrovou historii

2) Vyhnout se soudním sporům, placení poplatků a jiných soudních nákladů.

V případě prodlení uhrady pohledávky 9292.12 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_22365A830317939E.zip"

S pozdravem,

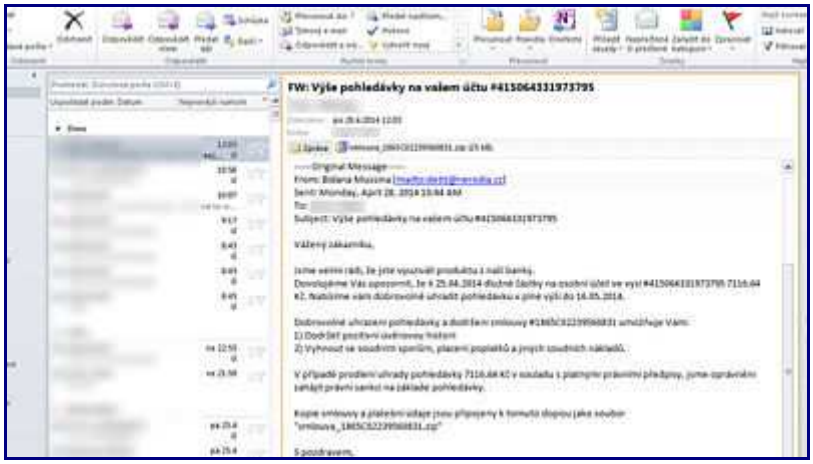
Vedoucí odboru vymahani pohledávek

Adam Bejšovec

Součástí e-mailu je i příloha, která má obsahovat údajnou smlouvu, jež dokazuje vznik dlužné částky. Místo toho se však v archívu ukrývá spustitelný soubor s koncovkou .exe, který kromě textového dokumentu ukrývá také počítačové viry.

„Přílohu, která obsahuje spustitelný soubor s koncovkou .exe by lidé v žádném případě neměli otevírat," varoval bezpečnostní analytik Pavel Bašta z týmu CSIRT, který je provozován sdružením CZ.NIC.

Podobně by lidé podle něj měli z preventivních důvodů postupovat i u dalších nevyžádaných e-mailů, které přicházejí z neznámých zdrojů.



Ukázka podvodného e-mailu.

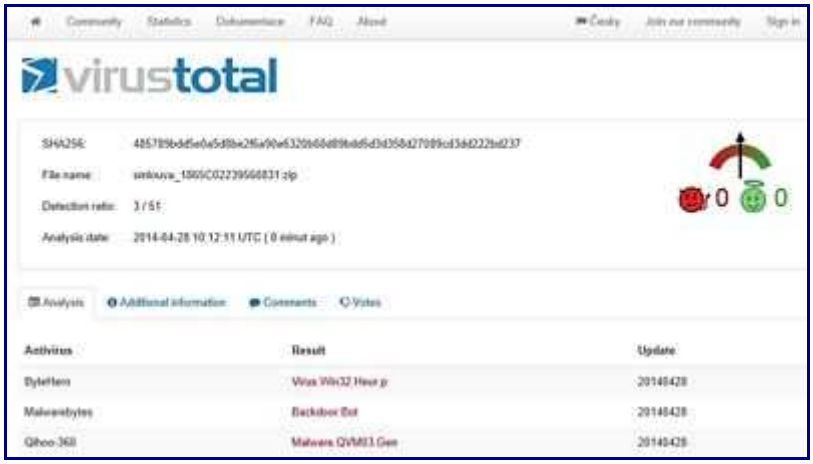
FOTO: Novinky

Některé antivirové programy s aktualizovanou virovou databází si dokážou s nezvanými návštěvníky poradit.

„Pokud jste již sobor nedopatřením spustili, podívejte se do adresáře Users/JMÉNO_UŽIVATELE/AppData/Roaming/brothel, pravděpodobně tam budete mít soubor ate.exe. Podle naší předběžné analýzy se jedná o soubor, který vznikne po spuštění přiloženého .exe souboru," konstatoval Bašta.

„Zároveň je v registrech vytvořen příslušný klíč ve větvi HKEY_CURRENT_USERSoftwareMicrosoftWindows CurrentVersionRun. Klíč i soubor je

potřeba smazat. Pokud by se to v normálním režimu nepodařilo, restartujte windows do nouzového režimu,“ poradil Bašta.



On-line nástroj Virus Total odhalil v infikovaném archívu hned tři různé hrozby.

FOTO: Novinky