Spear phishing

Pomáhat a chránit

KRAJSKÉ ŘEDITELSTVÍ POLICIE
JIHOMORAVSKÉHO KRAJE

Spear phishing … novinka na trhu aneb rybaření bez udic

Phishing (rybaření)
podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci

Zásadním rozdílem mezi obyčejným „phishingem“ a spear phishingem

phishingem

- zatímco běžný „RYBÁŘ“ používá návnadu… převedeno do naší problematiky, odešle odkaz, který láká například na aktualizaci programu, lepší zabezpečení internetového bankovnictví, nebo zaručenou výhru v soutěži.
- následně pak využívá získaných informací - přihlašovacích údajů
- znamená to, že musí vstoupit do emailu, do bankovnictví, aby pak dalším krokem dosáhl svého cíle

spear phishing

- zde na rozdíl od phishingu nepoužije „RYBÁŘ“ návnadu, ale útočí přímo harpunou (spear = kopí)
- nemusí čekat až se ryby chytí na návnadu, ale prostě vystřelí a buď se trefí, a nebo ne.
- zpravidla, ale nemíří na malé ryby, ale na velké kusy, = není většinou cílen na fyzické osoby, ale je zaměřen na firmy, a společnosti

- útočník si vybírá většinou ty společnosti, které jsou prezentovány na internetu (to jsou sice všechny)
- ale jeho hlavním cílem jsou právnické osoby, které mají veřejně dostupnou organizační strukturu

Spear phishing - Jak to vypadá v praxi ?

Útok má obvykle 3 fáze

Fáze č. 1

- u vybrané „ryby“ společnosti přijde email na ekonomické oddělení, nebo přímo paní účetní od „pana ředitele“ (našeho rybáře s harpunou)
- jednou větou dotáže na možnost provedení zahraniční platby v Eurech
- pohotová paní účetní, obratem odpovídá, popřípadě sdělí ještě i aktuální stav devizového konta

Fáze č. 2

- rybář = pan ředitel - střílí další „harpunu“ - v emailu posílá požadavek na zahraniční platbu
- jedná se vždy o zahraniční účet a výše platby je v rozmezí od 9.000,-EU do 130.000,-EU
- v emailu zasílá kompletní pokyny k odeslání platby, včetně i označení transakce Ta je označena např. jako „ Seminář, Administrativní seminář, Technologická infrastruktura Integrace softwaru, Branding a technologická infrastruktura, Elektrické stroje“ a
- požaduje zaslání potvrzení o uskutečněné platbě - fakturu doloží později… (nedoloží !!!)
- paní účetní peníze zpravidla (cca 30 % úspěšnost) peníze odešle

Fáze č. 3

- ryba zasažena
- peníze na účtu
- účetní spokojená jak rychle plní pokyny „šéfa“

P R O Z Ř E N Í

paní účetní už třetí den nemá od pana šéfa
fakturu, a tak zvedne telefon, a slušně požádá pana ředitele,
aby jí tu fakturu na 30.000,- EU, pro pana „ Aladina Aladina “ z Turecka donesl,
až půjde kolem - aby měla v účetnictví pořádek

z reakce pana ředitele,
ale následně usoudí, že
nikdy jí žádný takový email neposlal

Spear phishing – co následuje…

- banka – pokus o storno platby
- trestní oznámení na neznámého „hackera“, který asi hekl email pana ředitele

Co se vlastně stalo…

- takhle vypadá pravý email pana ředitele : reditel@veprin.cz
- tahle vypadá email zkušeného harpunáře : reditel@veprin.cz

Na první pohled 100 % shoda!

Spear phishing

Základní znaky:

- email založený na freemailové službě - zpravidla: AOL.com, Yandex.com, Post.com a další
- bankovní účty se neopakují je použit maximálně na dva útoky
- obsah emailu (googlština) pravopisné chyby - opakující se fráze
- emaily se navzájem liší - ale neustále se opakují různé kombinace stejných slov: docmail019, dnkmob, dnkpen, dkn.pen, reditel, officemail_001, ceoox, ceo.z …
- označení plateb: Seminář, Administrativní seminář, Technologická infrastruktura Integrace softwaru, Branding a technologická infrastruktura, Elektrické stroje
- na konci emailu se z 90% objevuje věta „ Odesláno z IPHONU“

Spear phishing

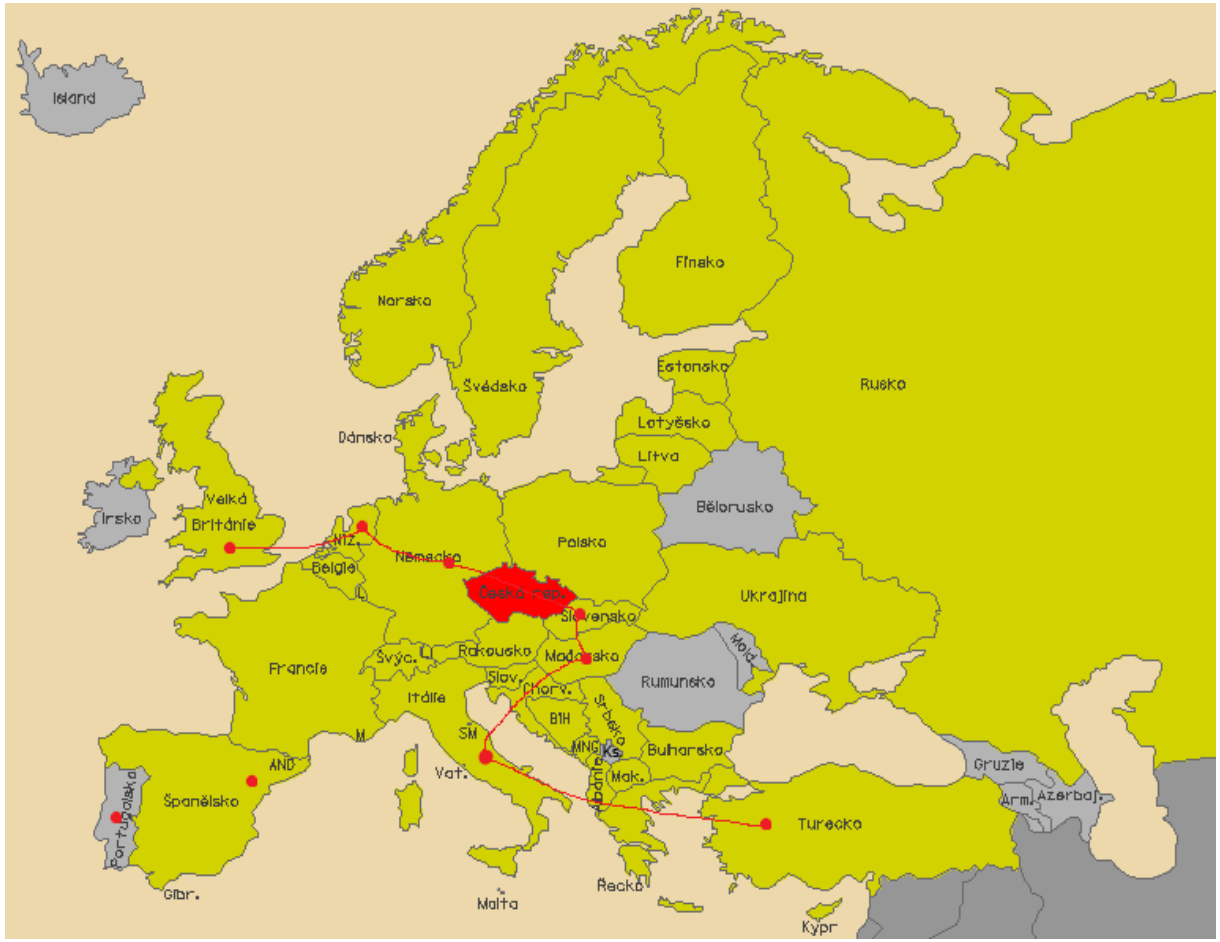
Jak se bránit…

- dobře nastavený spamový filtr - cca 75 % spolehlivost
- verifikace plateb ve firmě - 99 % spolehlivost
- používat rozum - 100 % spolehlivost

Právní kvalifikace

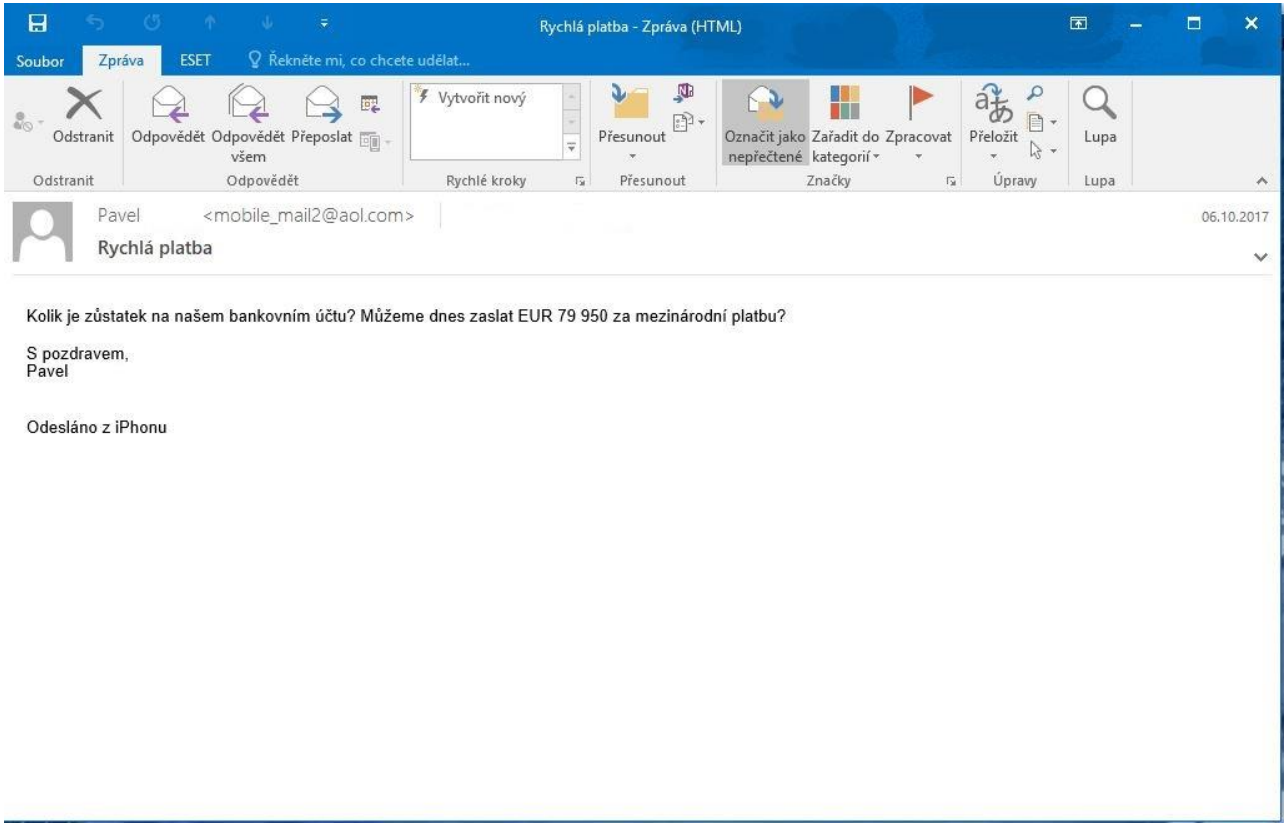
- § 209 podvod tr. zákoníku - při odeslání platby
- § 21 k § 209 pokus podvodu tr. zákoníku - v případě sdělení konkrétního bankovního účtu, na který má být platba realizována, ale nedojde k ní

Kde byly postupně zakládány bankovní účty

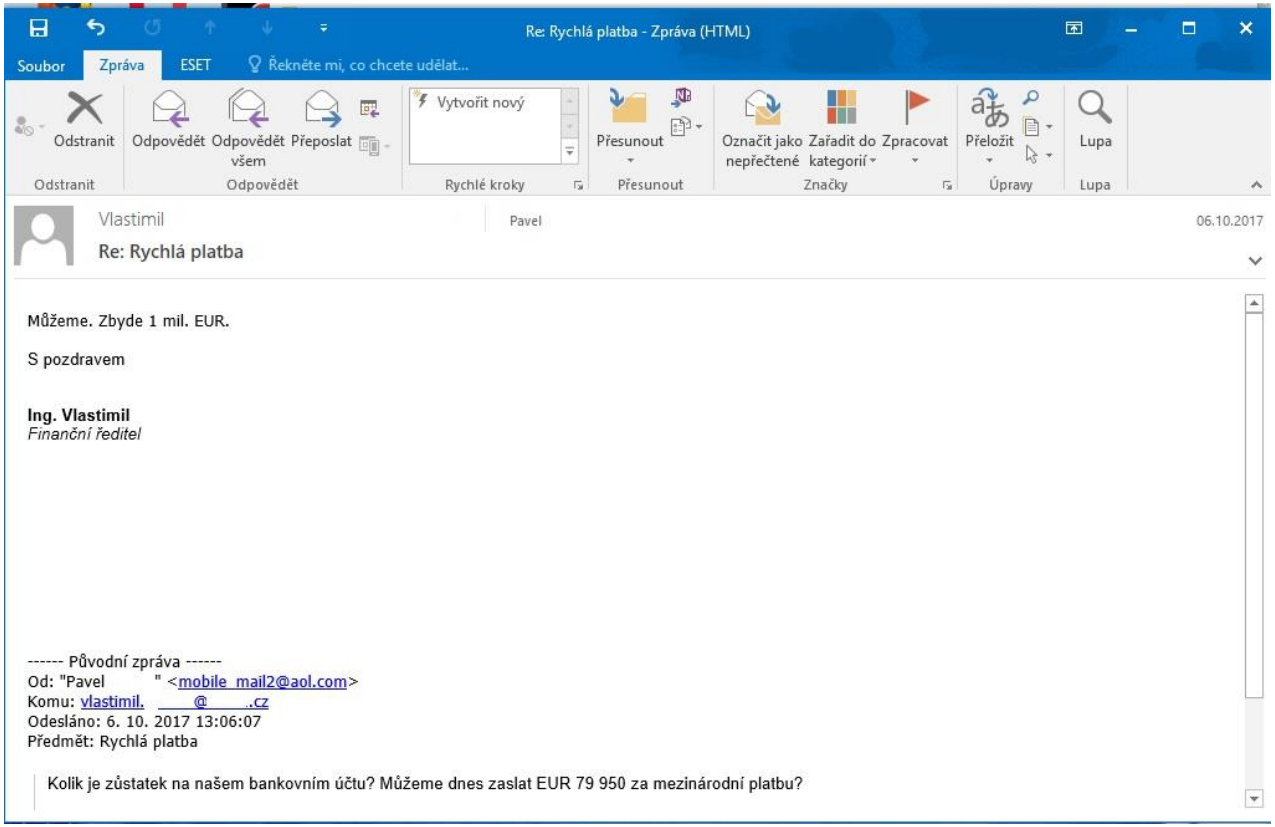


Turecko
Itálie
Španělsko
Portugalsko
Maďarsko
Slovensko
Německo
Nizozemí
Velká Británie

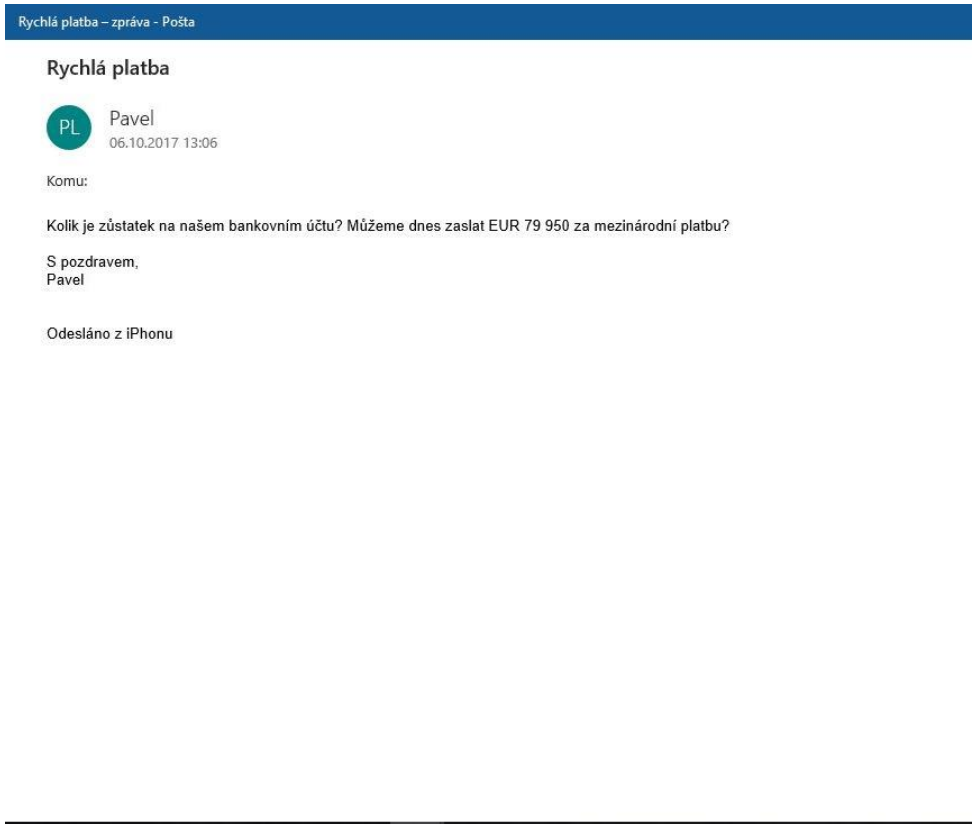
Podvrh


Rychlá platba - Zpráva (HTML)
Soubor
Zpráva
ESET
Řekněte mi, co chcete udělat...
Odstranit
Odpovědět
Odpovědět všem
Přeposlat
Vytvořit nový
Přesunout
Označit jako nepřečtené
Zařadit do kategorií
Zpracovat
Přeložit
Lupa
Odstranit
Odpovědět
Rychlé kroky
Přesunout
Značky
Úpravy
Lupa
Pavel <mobile_mail2@aol.com>
06.10.2017
Rychlá platba
Kolik je zůstatek na našem bankovním účtu? Můžeme dnes zaslat EUR 79 950 za mezinárodní platbu?
S pozdravem,
Pavel
Odesláno z iPhonu

Podvrh


Re: Rychlá platba - Zpráva (HTML)
Soubor
Zpráva
ESET
Řekněte mi, co chcete udělat...
Odstranit
Odpovědět
Odpovědět všem
Přeposlat
Vytvořit nový
Přesunout
Označit jako nepřečtené
Zařadit do kategorií
Zpracovat
Přeložit
Lupa
Odstranit
Odpovědět
Rychlé kroky
Přesunout
Značky
Úpravy
Lupa
Vlastimil
Pavel
06.10.2017
Re: Rychlá platba
Můžeme. Zbyde 1 mil. EUR.
S pozdravem
Ing. Vlastimil
Finanční ředitel
------ Původní zpráva ------
Od: "Pavel " <mobile_mail2@aol.com>
Komu: vlastimil. @ .cz
Odesláno: 6. 10. 2017 13:06:07
Předmět: Rychlá platba
Kolik je zůstatek na našem bankovním účtu? Můžeme dnes zaslat EUR 79 950 za mezinárodní platbu?

Podvrh



Rychlá platba – zpráva - Pošta

Rychlá platba

PL Pavel
06.10.2017 13:06

Komu:

Kolik je zůstatek na našem bankovním účtu? Můžeme dnes zaslat EUR 79 950 za mezinárodní platbu?

S pozdravem,
Pavel

Odesláno z iPhonu

Děkuji za pozornost

kpt. Mgr. Tomáš Němec