Jak a kde nahlásit spam českých firem?

Vložil/a cm3l1k1 [1], 3 Květen, 2010 - 13:20

- Security [2]
- Spam [3]

Určitě vám také několikrát do měsíce přijde "obchodní sdělení" od firmy, kterou neznáte a nemáte s ní nic společného. Mně už s podobnými alibisty došla trpělivost, a rozhodl jsem se, že od teď budu vše hlásit na ÚOOÚ (Úřad pro ochranu osobních údajů).
V tomto článku bych všem chtěl ukázat, jak postupovat a co je potřeba ověřit/zjistit.

Jak jsem se dozvěděl o postupu?

Nevěděl jsem na koho se obrátit, proto jsem zkusil napsat českému CSIRT teamu (Computer Security Incident Response Team) www.csirt.cz [4]
CSIRT teamy mají za úkol přinášet reaktivní a proaktivní činnost v oblasti zvládání počítačových incidentů. Jejich snahou je, pokud je to možné, incidentům předcházet nastavením vhodných protiopatření, přičemž pro CSIRT je nezbytná spolupráce s dalšími CSIRT, a to hlavně za účelem sdílení varování a znalostí (zkušeností).
Více v článku: CSIRT.cz - jak zvládnout bezpečnostní incidenty? [5]

Napsal jsem email, ve kterém jsem je seznámil s mým problémem. Mile mě překvapilo, s jakou rychlostí se mi dsotalo odpovědi (1 hodina). Požádali mě o kompletní hlavičku a tělo emailu, aby mohli rozhodnout, zda se opravdu jedná o nevyžádanou poštu.

Hlavička emailu (pozměněna, název firmy je však pravý):

```
Envelope-to: nekdo@nekde.cz
Received: from [xxxx] (helo=xxxx)
        by xxxx with esmtp (Exim 4.69)

        (envelope-from <info@normy.cz>)
        id 1O4uVU-0000xa-DP
        for nekdo@nekde.cz; Thu, 22 Apr 2010 13:23:44 +0200
Received: from mail.login.cz ([193.86.200.20] helo=fs.spinet.cz) by

        xxxx with ESMTP (2.0.1); 22 Apr 2010 13:23:38 +0200
Received: from localhost (localhost [127.0.0.1])
        by fs.spinet.cz (Postfix) with ESMTP id 5F2ED38ECB0

        for <nekdo@nekde.cz>; Thu, 22 Apr 2010 13:23:37 +0200 (CEST)
X-Virus-Scanned: Debian amavisd-new at spinet.cz
Received: from fs.spinet.cz ([193.86.200.20])

        by localhost (fs.spinet.cz [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id hxP5lALXh8oa for <nekdo@nekde.cz>;

        Thu, 22 Apr 2010 13:23:29 +0200 (CEST)
Received: from WIN-8093KC2FHC7 (unknown [193.86.200.72])
        by fs.spinet.cz (Postfix) with ESMTP id 84977B2AB48
        for <nekdo@nekde.cz>; Tue, 20 Apr 2010 21:30:06 +0200 (CEST)
```

```
MIME-Version: 1.0
From: info@normy.cz
To: nekdo@nekde.cz
Date: 20 Apr 2010 21:30:00 +0200
Subject: =?utf-8?B?Tm9ybXkuY3ogLSDFvsOhZG9zdCBvIHNvdWhsYXMgc2UgemFzw61sw6Fuw61tIG9iY2
hvZG7DrWNoIHNkxJtsZW7DrQ==?=

Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
Message-Id: <20100420193006.84977B2AB48@fs.spinet.cz>
X-Assp-Message-Score: 10 (Bad IP History)

X-Assp-Received-SPF: pass ip=193.86.200.20 mailfrom=info@normy.cz
        helo=fs.spinet.cz
X-Assp-Message/IP-Score:=?UTF-8?Q?=20?=-5 (SPF pass)
X-Assp-Envelope-From: info@normy.cz

X-Assp-Intended-For: nekdo@nekde.cz
```

Tělo emailu:

```
Dobrý den,

v souladu s ust. § 7 zákona ?. 480/2004 Sb., o n?kterých službách
informa?ní spole?nosti, ve zn?ní pozd?jších p?edpis?, si Vás
dovolujeme požádat o souhlas se zasíláním obchodních sd?lení
s nabídkou našich služeb týkajících se technických norem, informa?ních
a dalších služeb s nimi spojených.

V p?ípad?, že souhlasíte se zasíláním obchodních sd?lení s uvedeným obsahem, klikn?te
laskav? na tento odkaz

http://www.normy.cz/zajem-s.aspx?email=nekdo@nekde.cz&bn=1

Souhlas lze kdykoliv jednoduše odvolat zasláním e-mailu s žádostí
o zrušení souhlasu nebo p?ípadn? kliknutím na p?íslušný odkaz, pokud je sou?ástí
zaslaného sd?lení.

Pokud nesouhlasíte, klikn?te na níže uvedený odkaz a Vaše e-mailová adresa bude
vymazána z naší databáze

http://www.normy.cz/nezajem-s.aspx?email=nekdo@nekde.cz

D?kujeme
S p?áním hezkého dne
Ing. Jan Jelínek
e-Business Services a.s.
divize Normy.CZ
www.normy.cz
```

SPAM jako řemen!

Alibistický postoj se zakoníkem a převrácením smyslu e-mailu, jakožto prostředku dotázání se, zda mi mohou posílat reklamní emaily, mě dokáže naštvat.
Předně: Již tento e-mail je klasifikován jako spam!

Mohou mi zasílat e-maily na základě mé přímé žádosti. Tj. já bych musel takový krok odsouhlasit, nebo podepsat apod. Jednoduše: Muselo by se jednat o aktivní zájem z mé strany.

Spamy takového charakteru chodí od velké spousty společností, které na takové jednání mají žaludek (banan.cz už nikoho nepřekvapí).

Jak ověřit, že email zaslala daná společnost?

Pokud dokážeme, že se jedná o e-mailovou zprávu, která byla zaslána ze serverů společnosti, jedná se o nepopíratelný důkaz, který je potřeba pro případný další postup.
I když použijí cizí SMTP server, případně využijí služeb hromadného rozesílání e-mailu, je i tak možné dohledat původce e-mailů. Jen to ÚOOÚ zabere o něco více času.

Z hlavičky mailu se můžeme dozvědět, že mail byl zaslán serverem:

```
Received: from WIN-8093KC2FHC7 (unknown [193.86.200.72])
        by fs.spinet.cz (Postfix) with ESMTP id 84977B2AB48
        for <nekdo@nekde.cz>; Tue, 20 Apr 2010 21:30:06 +0200 (CEST)
```

Je to poslední header "Received:" v hlavičce mailu (protože další SMTP servery dávají svůj záznam vždy na začátek). Takže podle hostname **fs.spinet.cz** lze usuzovat, že email byl zaslán serverem společnosti SPINET.

Podíváme se, kde je normy.cz hostován:

```
deuterius:~ mc$ host normy.cz
normy.cz has address 193.86.200.72
normy.cz mail is handled by 50 login.cz.
normy.cz mail is handled by 100 lvs1.spinet.cz.
```

Již nyní vidíme propojení s firmou SPINET. Oveříme to dotazem na WHOIS

```
inetnum:      193.86.192.0 - 193.86.207.255
netname:      SPINET
descr:        SPINET, Inc.
descr:        Prague
country:      CZ
admin-c:      LS5-RIPE
tech-c:       JK30-RIPE
status:       ASSIGNED PA
mnt-by:       GTSCZ-MNT
source:       RIPE # Filtered
```

OK, Normy.cz hostují u SPINET, přičemž mail byl také z těchto serveru zaslán.

Přejdeme na web ÚOOÚ, kam nás odkázali lidé z CSIRT.CZ

Nahlášení spamu

URL webu: http://www.uoou.cz/uoou.aspx?menu=23&submenu=27 [6]
Přímý link na formulář: http://www.uoou.cz/uoou.aspx?menu=23&submenu=27&loc=464 [7]

Zde vyplníme všechny potřebné údaje, jako např.
» Forma spamu (mail, fax, sms)
» Hlavička emailu
» Tělo emailu
» Kontaktní údaje

Po dokončení máte ještě možnost si vámi vyplněný incident stáhnout jako PDF a čekat na odpověď úřadu.

Zaregistroval jsem incident přibližne před týdnem a zatím nemám odpověd.
Po obdržení odpovědi budu o dalším postupu dále informovat.

Nyní tedy již víte jak spam ohlásit a nic vám nebrání v nahlášení ostatních firem konající tyto podvodné praktiky.

V současnosti nás stovky spamů denně moc netrápí. Většinu totiž zachytí poměrně sofistikované antispamy. Český spam však těmto scannerům uniká, protože se jedná o celosvětově bezvýznamný podíl zpráv, navíc psaný naší mateřštinou.

URL článku:
https://security-portal.cz/clanky/jak-kde-nahl%C3%A1sit-spam-%C4%8Desk%C3%BDch-firem

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/security
[3] https://security-portal.cz/category/tagy/spam
[4] http://www.csirt.cz
[5] https://security-portal.cz/clanky/csirtcz-jak-zvládnout-bezpečnostní-incidenty
[6] http://www.uoou.cz/uoou.aspx?menu=23&submenu=27
[7] http://www.uoou.cz/uoou.aspx?menu=23&submenu=27&loc=464