

Spam: vývoj a dopad

Spam, lovely spam, wonderful spam.

Miloslav Cahlík

18. února 2009

Co všechno na sebe povíme?

Return-Path: tomas.jedno@domena.net

Received: from gw.domena.net ([192.168.1.253]) by gw2.domena.net for taky.jedno@domena.net; Mon, 1 Sep 2008 10:42:54 +0200

Received: from gw2.domena.net ([XXX.XXX.XXX.XXX]) by exgw.domena.cz for < taky.jedno@domena.net >; Mon, 01 Sep 2008 09:59:48 +0200

Received: from exgw.domena.local (192.168.2.252) by smtp1.domena.cz (10.0.2.23) with Microsoft SMTP Server (TLS) id 8.1.278.0; **Exchange Server 2007 SP1**

Received: from EXCHANGE.domena.local ([192.168.2.93]) by exgw.dmena.local ([192.168.2.252]) with mapi; Mon, 1 Sep 2008 10:41:47 +0200 From: =Tomas Jedno < tomas.jedno@domena.cz >

Date: Mon, 1 Sep 2008 10:41:44 +0200 Subject: ITIL Thread-Topic: ITIL Thread-Index: AckMDpARuCr3k8rnSpOmHc99/1c+BA== Message-ID: <084EE0E5D0DB874F8A69418587CF7DF20A2690CD@EXCHANG E.domenalocal>

Co všechno na sebe povíme?

Sociální sítě

55 % náctiletých vytvořilo svůj osobní profil na internetu

66% těchto lidí tvrdí, že jejich celý profil není veřejně dostupný

70% dívek na rozdíl od 54% chlapců starších 17 let používá sociální síť

70% dívek starších 17 let si vytvořilo svůj profil hned po té, co tak učinil MMP

Chování náctiletých v sociálních sítích

	ano	ne
Zůstávají v kontaktu s přáteli často se stýkají	91%	9%
Zůstávají v kontaktu s přáteli, které málo vidí	82%	18%
Plánují společně s přáteli	72%	28%
Hledají nové přátele	49%	51%
Flirtují mezi sebou	17%	83%

Zdroj: Pew internet & American Life Project Parents & Teens Survey, October-November 2006. Base on teens who use social networking site. Margin of error is $\pm 5\%$.

Co všechno na sebe povíme?

jméno:		příjmení:	
pohlaví:	Žena	e-mail:	
ulice:		č. p.:	
město:		PSC:	
země:	Česká Republika	datum narození:	
počet osob v domácnosti:	0		<i>formát (den. měsíc. rok)</i>
telefon:		datum svátku:	
jsem těhotná:	☐		<i>formát (den. měsíc.)</i>
Uvedte prosím, odkud jste se dozvěděla o našich stránkách:			
☐ Porodnice - materiály v Klinikboxu			
☐ Internet			
☐ Lékárna			
☐ Pediatr			
☐ Kamarádka, uveďte její nick:			
☐ Hami Jídelníček			
☐ Jinak, uveďte jak:			
Údaje o Vašich dětech			
počet dětí:	-		

Hoax – využití touhy lidí po senzacích

- **"Obama refused to be the president of the United States of America"** Obama se odmítl stát prezidentem USA – [trojský kůň](#)
- **Samoodpočet elektřiny – důležité** – [poplašná zpráva – poškození pověsti dodavatele energie](#)
- **Šteniatka Retrieverov a Labradorov** – [rozesílání lživé informace o týrání zvířat – senzace / skandál](#)
- **ICE kontakty v mobilu - In Case of Emergency** – [hromadný email](#)
- **Nevolejte 09, 9090, # 90 nebo #09** – [poplašná zpráva](#)

Zdroj: www.hoax.cz

Phishing v dějinách

Izák řekl: „Hle, jsem už starý a neznám den své smrti. Vezmi si nyní zbraně, toulec a luk, vyjdi na pole a něco pro mě ulov. Připrav mi oblíbenou pochoutku a přines mi ji, ať se najím, abych ti mohl požehnat, dříve než umřu.“ ..

.. Jákob však své matce Rebece odvětil: „**Můj bratr Ezau je přece chlupatý, a já jsem holý.** Co když si otec na mě sáhne? Bude mě mít za podvodníka a místo požehnání na sebe uvedu zlořečení.“ ..

.. I vešel k svému otci a řekl: „**Můj otče!**“ On odvětil: „Tu jsem. Který jsi ty, můj synu?“ Jákob řekl otci: „**Já jsem Ezau, tvůj prvorozený.** Učinil jsem, co jsi mi uložil. ..

.. “Izák řekl Jákobovi: „Přistup, synu, sáhnu si na tebe, jsi-li můj syn Ezau nebo ne.“ Jákob tedy přistoupil k svému otci Izákovi, on na něho sáhl a řekl: „**Hlas je to Jákobův, ale ruce jsou Ezauovy.**“ **Nepoznal ho, protože jeho ruce byly chlupaté jako ruce jeho bratra Ezaua.** A požehnal mu.

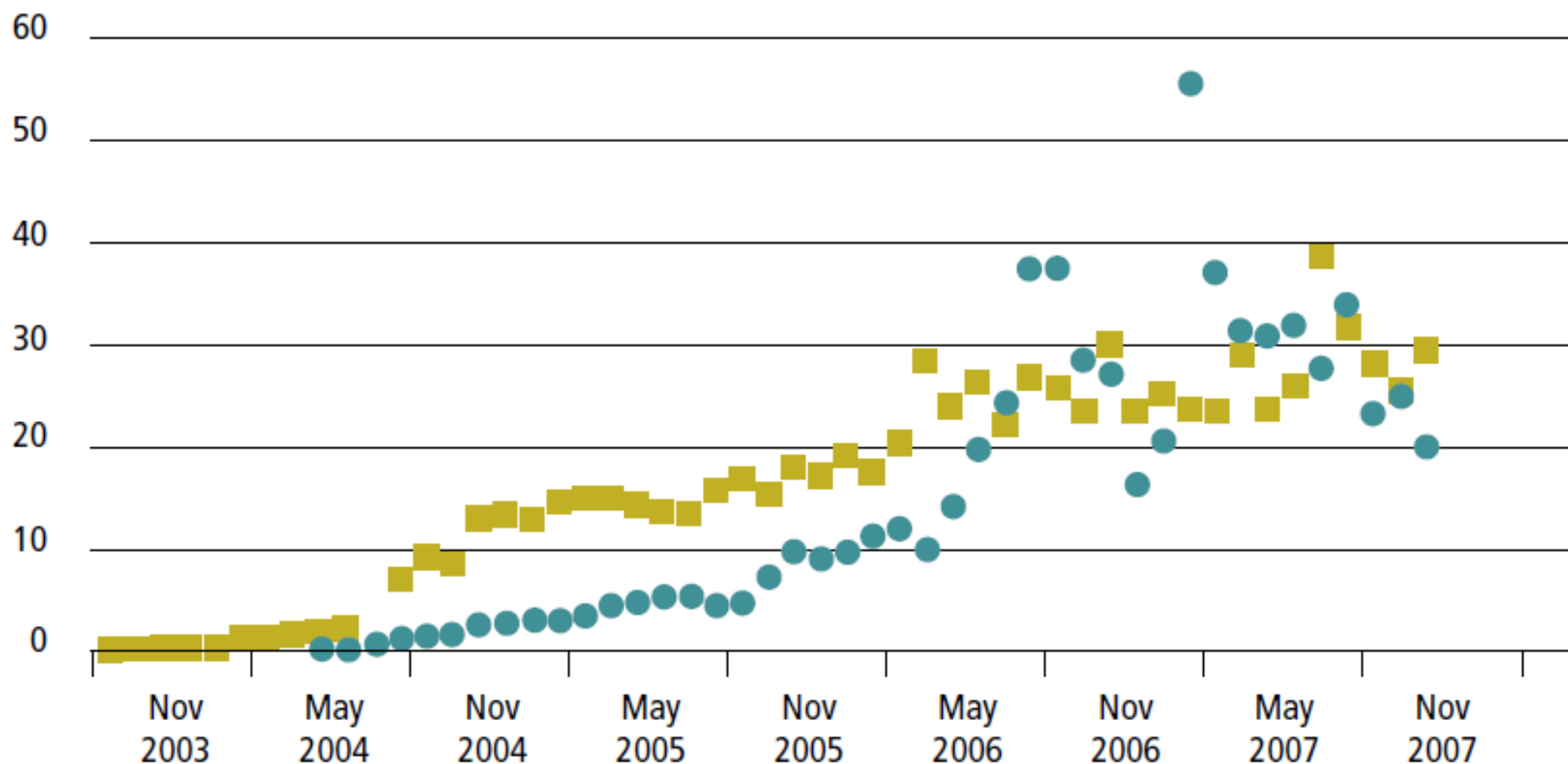
Genesis 27, 2 ~ 23

Phishing v blízké minulosti

Phishing reports

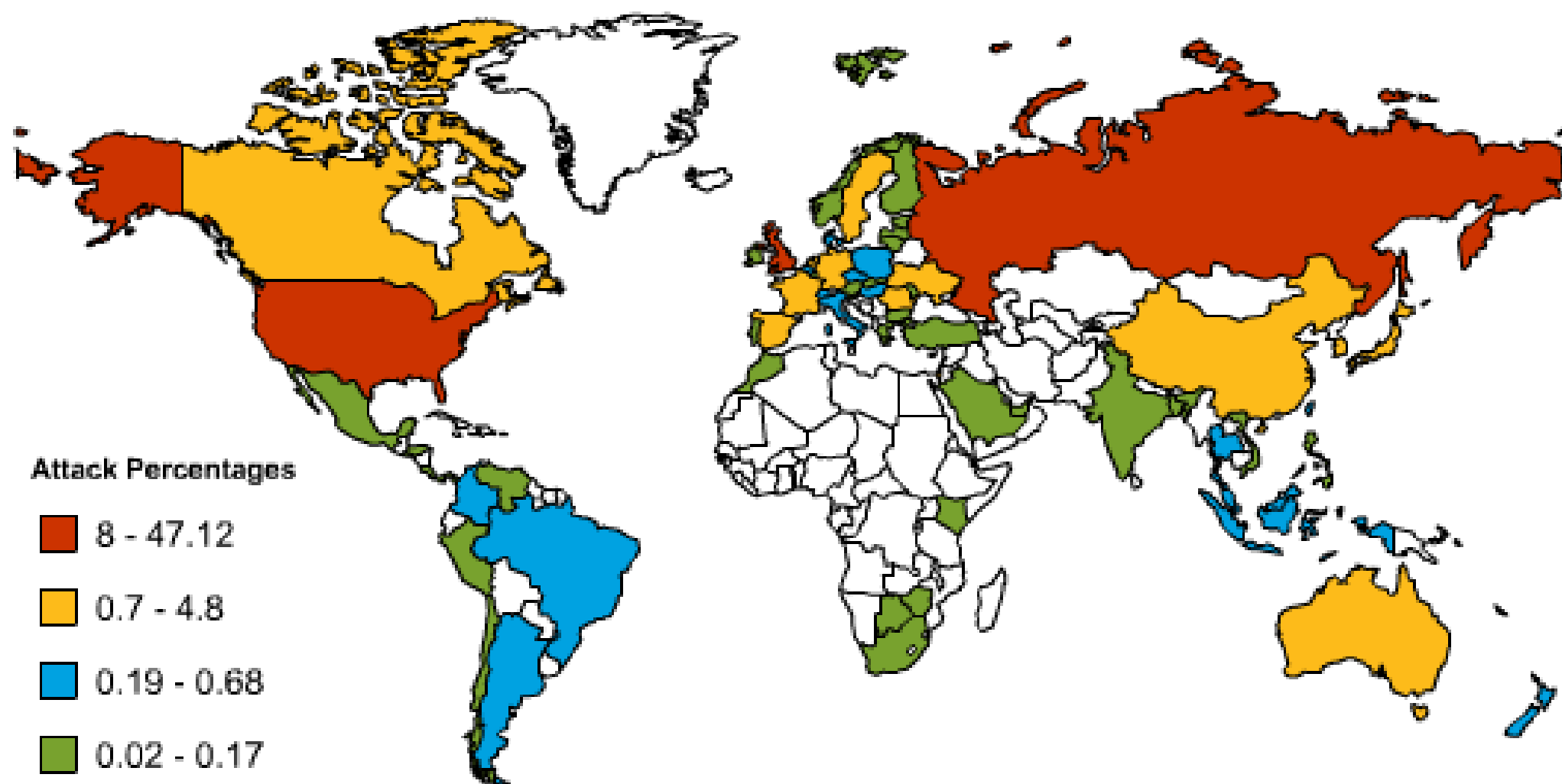
In thousands

- Unique phishing reports
- New phishing sites



Zdroj: McAfee, Inc., www.apwg.org

Phishing v 3. týdnu roku 2009



Zdroj: www.apwg.org

Social Engeneering

- Pornografické odkazy a obrázky
- Politické problémy, diskuze, kandidáti na prezidenta apod.
- Podvržené emaily z bankovních institucí.
- Programy zdarma, bezpečnostní nástroje.
- Velké události (olympijské hry, přírodní katastrofy apod.)
- Zneužití jmen, fotek celebrit.
- Potencionálně „důvěrné weby“ sociálních sítí

Shrnutí

Příčiny:

- nevědomost
- zvědavost
- touha po pikantnostech
- závist



Důsledky:

- osobní údaje veřejně přístupné
- snížená produktivita (nejen) práce
- příživnictví na lidské hlouposti a neštěstí
- zaplněné schránky (nejenom elektronické)

Spam, lovely spam, wonderful spam.



Spam, lovely spam, wonderful spam.

První spam - 1978: The first internet E-mail spam, sent by DEC

Einar Stefferud, a longtime net hand, reports that DEC announced a new DEC-20 machine in 1978 by sending an invite to **all ARPANET addresses (393 recipients) on the west coast**, using the ARPANET directory, **inviting people to receptions in California**. They were chastised for breaking the ARPANET appropriate use policy, and a notice was sent out reminding others of the rule.

Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT

Date: 1 May 1978 1233-EDT

From: THUERK at DEC-MARLBORO

Subject: ADRIAN@SRI-KL

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM

HYATT HOUSE (NEAR THE L.A. AIRPORT)

LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM

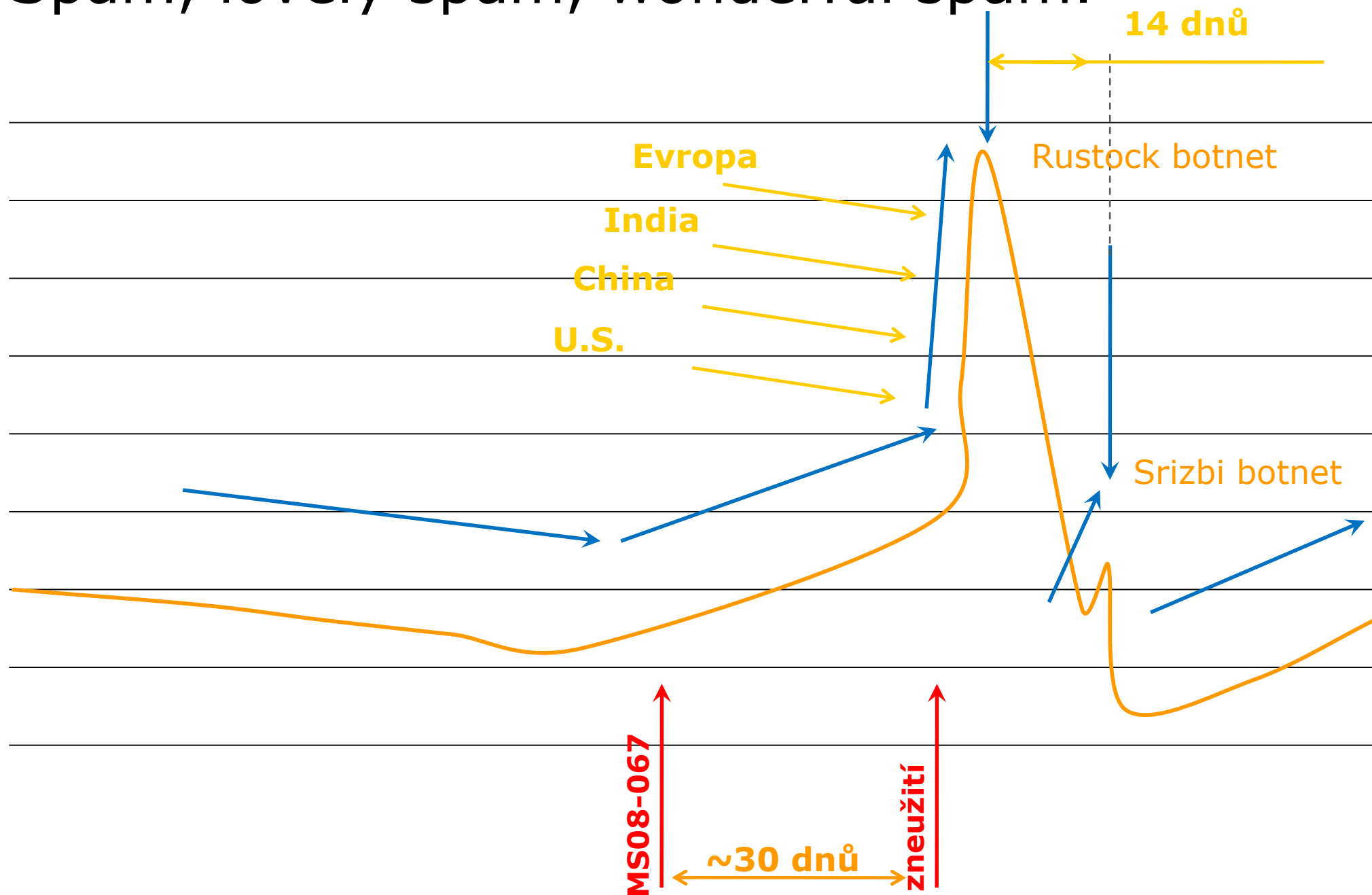
DUNFEY'S ROYAL COACH

SAN MATEO, CA

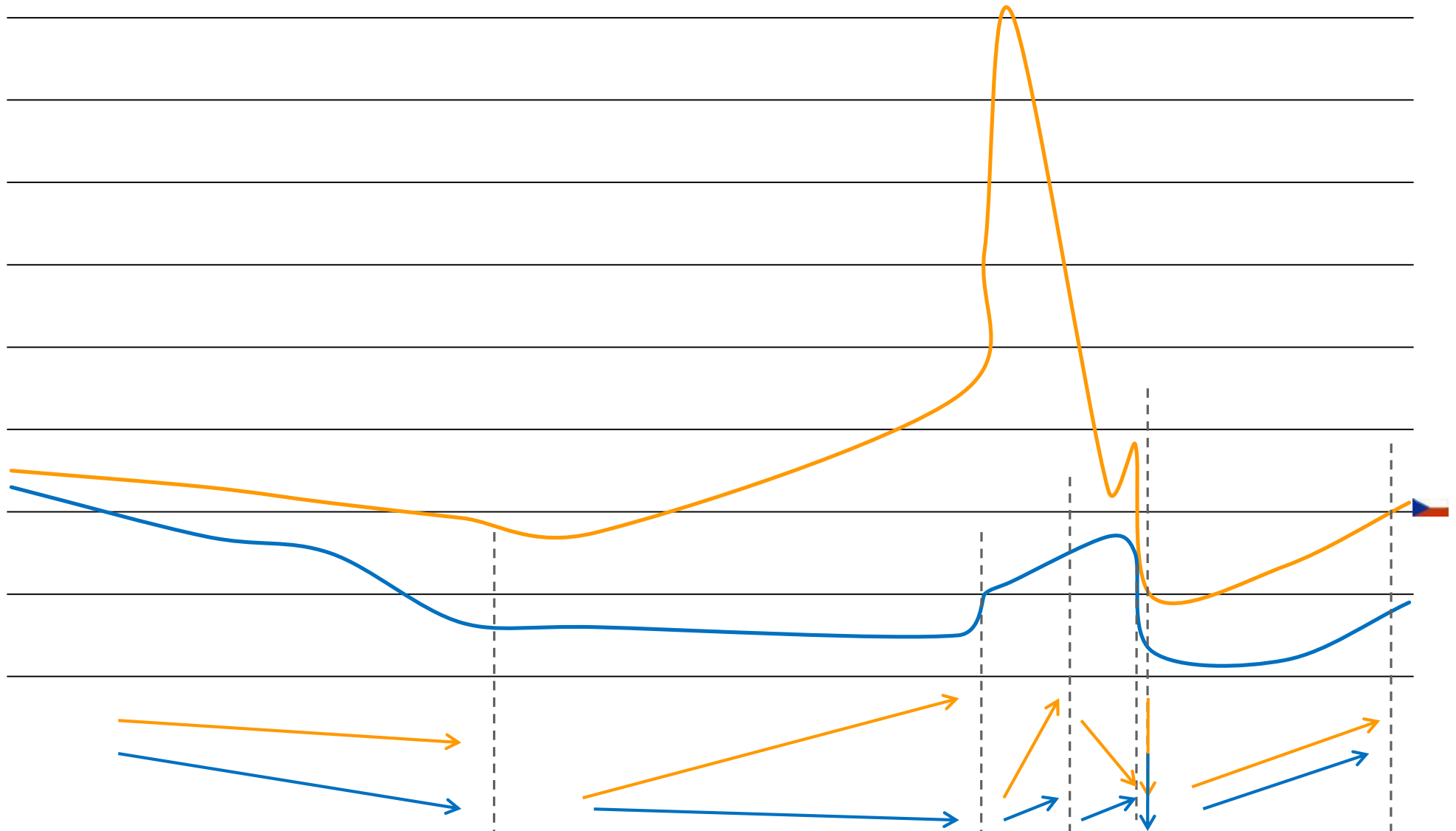
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

Spam, lovely spam, wonderful spam.



Spam, lovely spam, wonderful spam.



MS08-067 – vztah škodlivého kódu a spamu

23. 10. 2008

Vendor has provided a patch.

23. 10. 2008

A proof of concept has been released.

24. 10. 2008

Exploit code has been released.

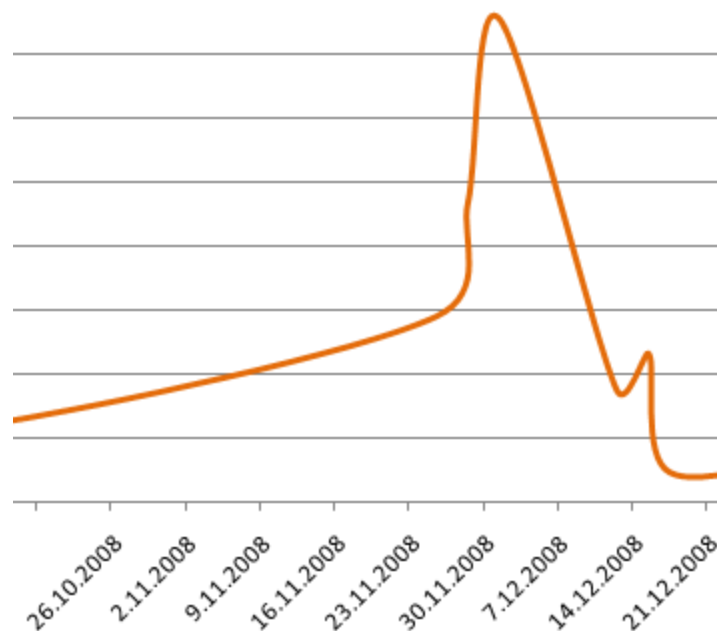
Zranitelné systémy:

Windows 2000 SP4,
Windows XP SP3,
Windows XP X64 SP2,
Windows 2003 SP2,
Windows 2003 x64 SP2,
Windows 2003 Itanium SP2,
Windows Vista SP1,
Windows Vista X64 SP1,
Windows 2008.

Vulnerability in Server Service Could Allow Remote Code Execution

Worm:Win32/Conficker.A (Microsoft)
Crypt.AVL (AVG)
Mal/Conficker-A (Sophos)
Win32/Conficker.worm (McAfee)
Trojan.Win32.Pakes.lxf (F-Secure)
Trojan.Win32.Pakes.lxf (Kaspersky)
W32.Downadup (Symantec)
Worm:Win32/Conficker.B (Microsoft)
WORM_DOWNAD.A (Trend Micro)

24. 11. 2008 ~100 000 infikovaných PCs



Spam, lovely spam, wonderful spam.

ochrana proti DoS útokům

IP defender

Black/White listy

Greylisting, SPF, Domain Key, Caller ID

Kontrola DNS

Detekce spamu z botnet sítí

Antivirové motory

Filtrování nechtěných příloh emailů

Filtrování nechtěného obsahu emailů

Uživatelské filtry

Kontrola detekčními vzorky

Kontrola obrázků Matrix Twins

Kontrola obsahu dokumentů

Bayesiánská analýza

Vyhodnocení: spam/ham

**Kontrola
odesílatele**

**Antivirová
kontrola**

**Kontrola
obsahu**

Spam, lovely spam, wonderful spam.

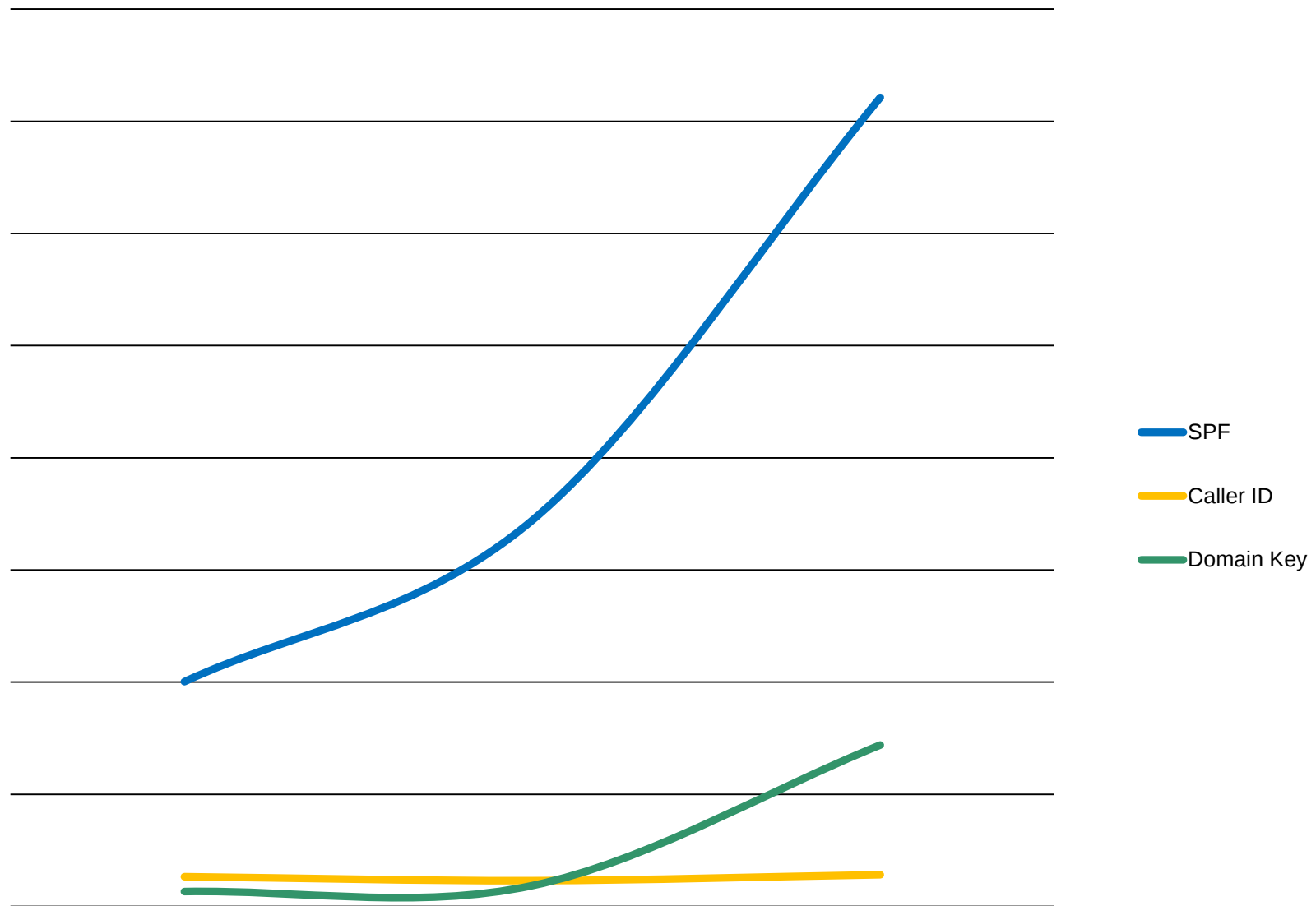
Metoda	Použití
Filtrování nechtěného obsahu emailů	exaktní slova: <i>viagra</i> <i>rollex</i>
Uživatelské filtry	slova a slovní spojení: <i>v agra</i> <i>vi@gra</i> <i>ro ex</i> <i>r0llex</i> kombinace slovních spojení, detekce prvků v emailu
Kontrola detekčními vzorky	složitě kombinace slovních spojení, detekce prvků ve zdrojovém kódu emailů, kontrola struktury celé datové zprávy
Kontrola obrázků	detekce jednoduchých typů obrázkového spamu
MatrixTwins	detekce obrázků různě strojově změněných (např. šumem, posunem či rotováním, změnou barev písma, atd..)
Kontrola obsahu dokumentů	detekce spamů v různých typech příloh jako např. ve formátu .pdf
Bayesiánská analýza	matematická analýza vyhodnocující pravděpodobnost s jakou je daný email spam, či legitimní email

Spam, lovely spam, wonderful spam.

- **Analýza struktury emaily**

- **Detekce spamu na základě otisku zprávy – hash**

.cz Statistika – SPF, Caller ID, Domain Key



Spam, lovely spam, wonderful spam.

Budoucnost?

Šifrované emaily – využívání certifikátů z certifikačních autorit

Zasílání přes **legitimní emailové servery**

Mohutné vytváření **botnet** sítí a jejich využití pro šíření spamu

Spam v konferencích, webových komentářích, mobilní technologie...

...

...

...

...

...

...

...

Závěrem

