

Joint Internet Society, CITEEL and ITU

Workshop on Combating SPAM

(Mendoza, Argentina, 7 October 2013)

Rethinking Spam The Evolution of a Threat Vector

Paul J.S. Oliveria

Security Focus Lead, Trend Micro

Paul_Oliveria@trendmicro.com

On a typical day, Trend Micro identifies...

>170M
spammed
messages



Web Reputation

17K
new malicious
URLs

TrendLabs
MULTI-THREAT
CORRELATION



Email Reputation

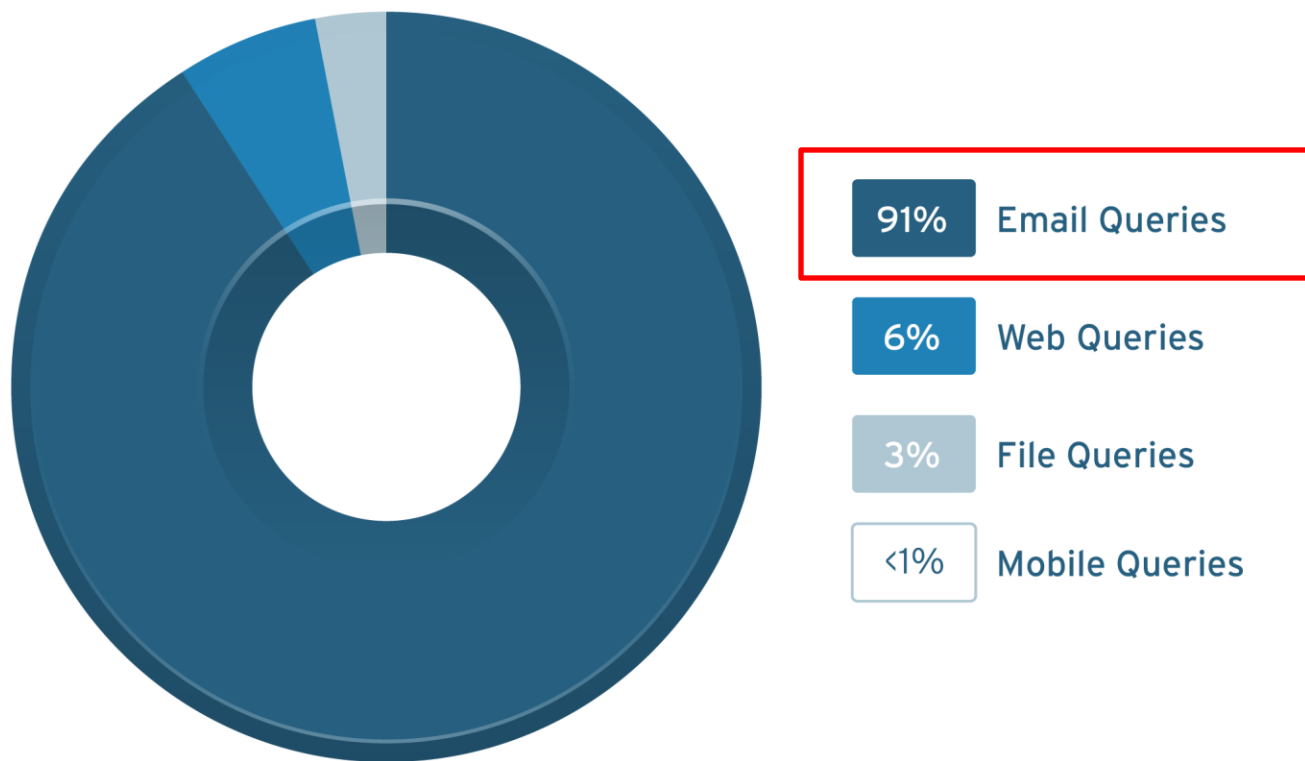


File Reputation

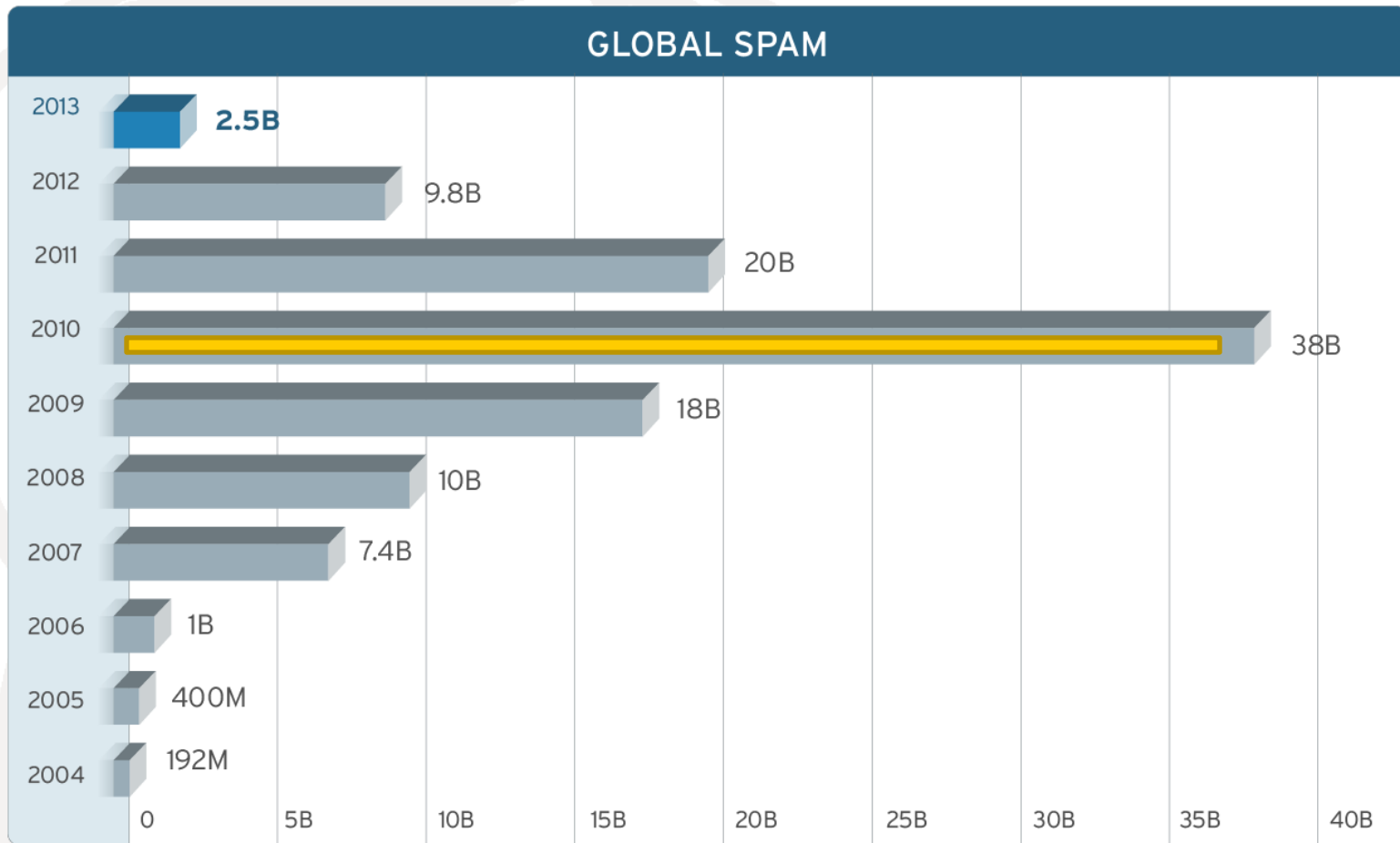
4.2M
malicious files

Email is BULK of malicious activities

CONFIRMED MALICIOUS ACTIVITIES DETECTED IN 2012



Massive impact of BOTNET TAKEDOWNS



Spam is GLOBAL

2012 TOP 10 SPAM-SENDING COUNTRIES

①	India	13%
②	Saudi Arabia	8%
③	United States	6%
④	South Korea	4%
⑤	Peru	4%
⑥	Vietnam	4%
⑦	Turkey	4%
⑧	Brazil	4%
⑨	Russia	3%
⑩	Indonesia	2%
	Others	49%
	TOTAL	100%

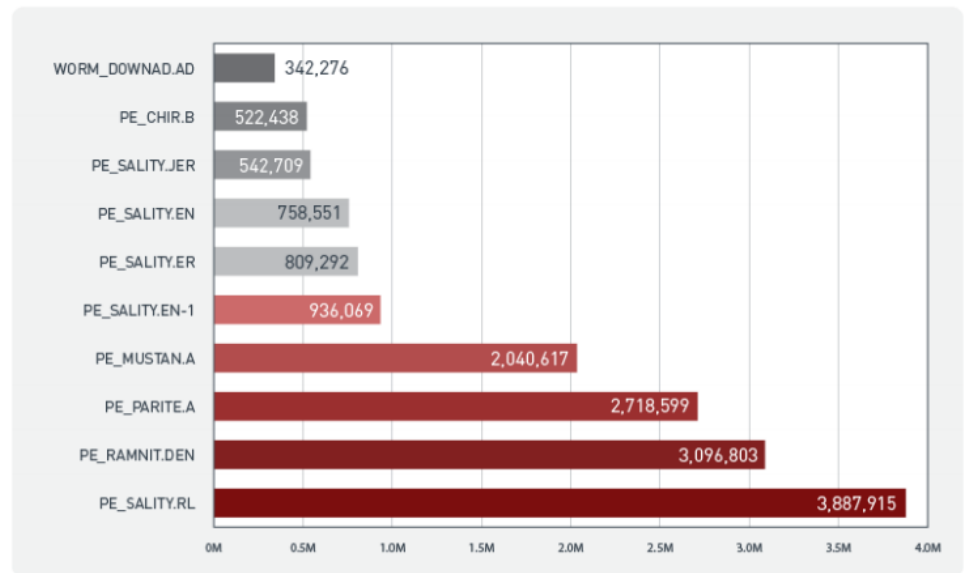
2012 TOP 10 SPAM LANGUAGES

①	English	88.64%
②	Russian	2.03%
③	Italian	1.59%
④	Japanese	1.39%
⑤	Chinese	0.97%
⑥	German	0.61%
⑦	Portuguese	0.26%
⑧	Spanish	0.22%
⑨	Slovak	0.20%
⑩	French	0.09%
	Others	4.01%
	TOTAL	100%

LAR is not immune




Top 10 Malware in the Americas and the Caribbean in 2012



Source: Trend Micro™ Smart Protection Network™

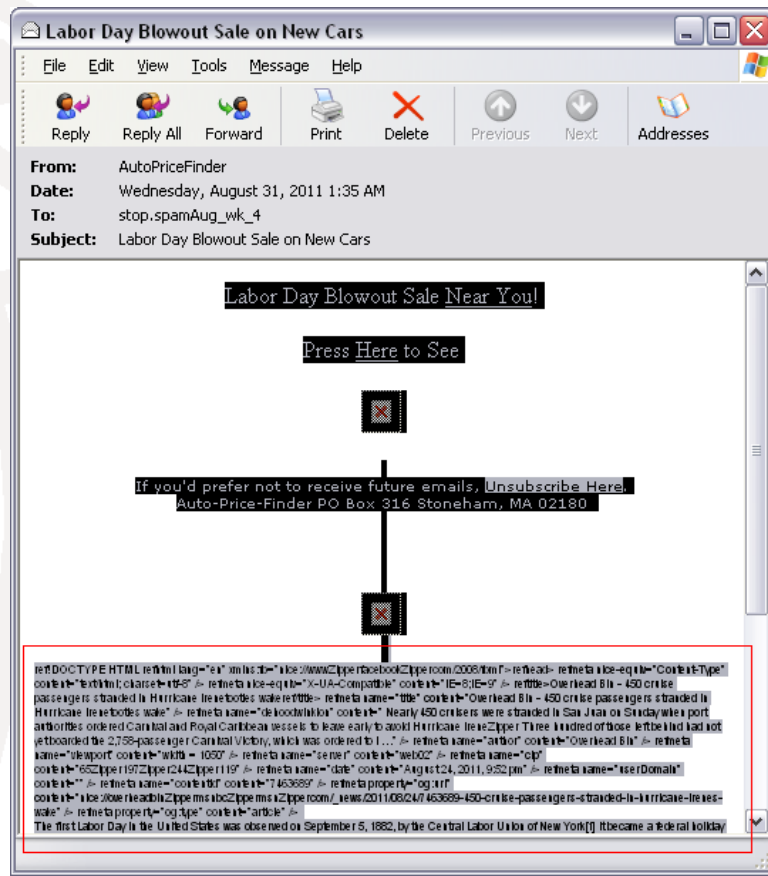
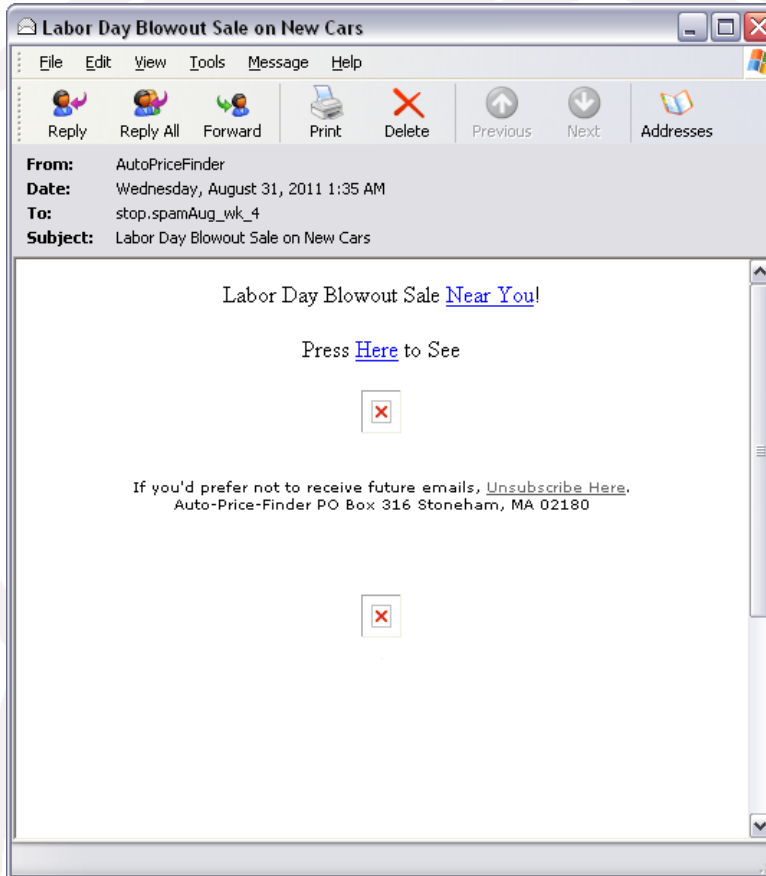
Spamming as a Service (SaaS)

OFFERING	PRICE
• Cheap email spamming service	US\$10 per 1,000,000 emails
• Expensive email spamming service using a customer database	US\$50-500 per 50,000-1,000,000 emails
• SMS spamming service	US\$3-150 per 100-10,000 text messages
• ICQ spamming service	US\$3-20 per 50,000-1,000,000 messages
• 1-hour ICQ flooding service	US\$2
• 24-hour ICQ flooding service	US\$30
• Email flooding service	US\$3 for 1,000 emails
• 1-hour call flooding service (i.e., typically takes call center services down)	US\$2-5
• 1-day call flooding service	US\$20-50
• 1-week call flooding service	US\$100
• SMS flooding service	US\$15 for 1,000 text messages
• Vkontante.ru account database	US\$5-10 for 500 accounts
• Mail.ru address database	US\$1.30-19.47 per 100-5,000 addresses
• Yandex.ru address database	US\$7-500 per 1,000-100,000 addresses
• Skype SMS spamming tool	US\$40
• Email spamming and flooding tool	US\$40



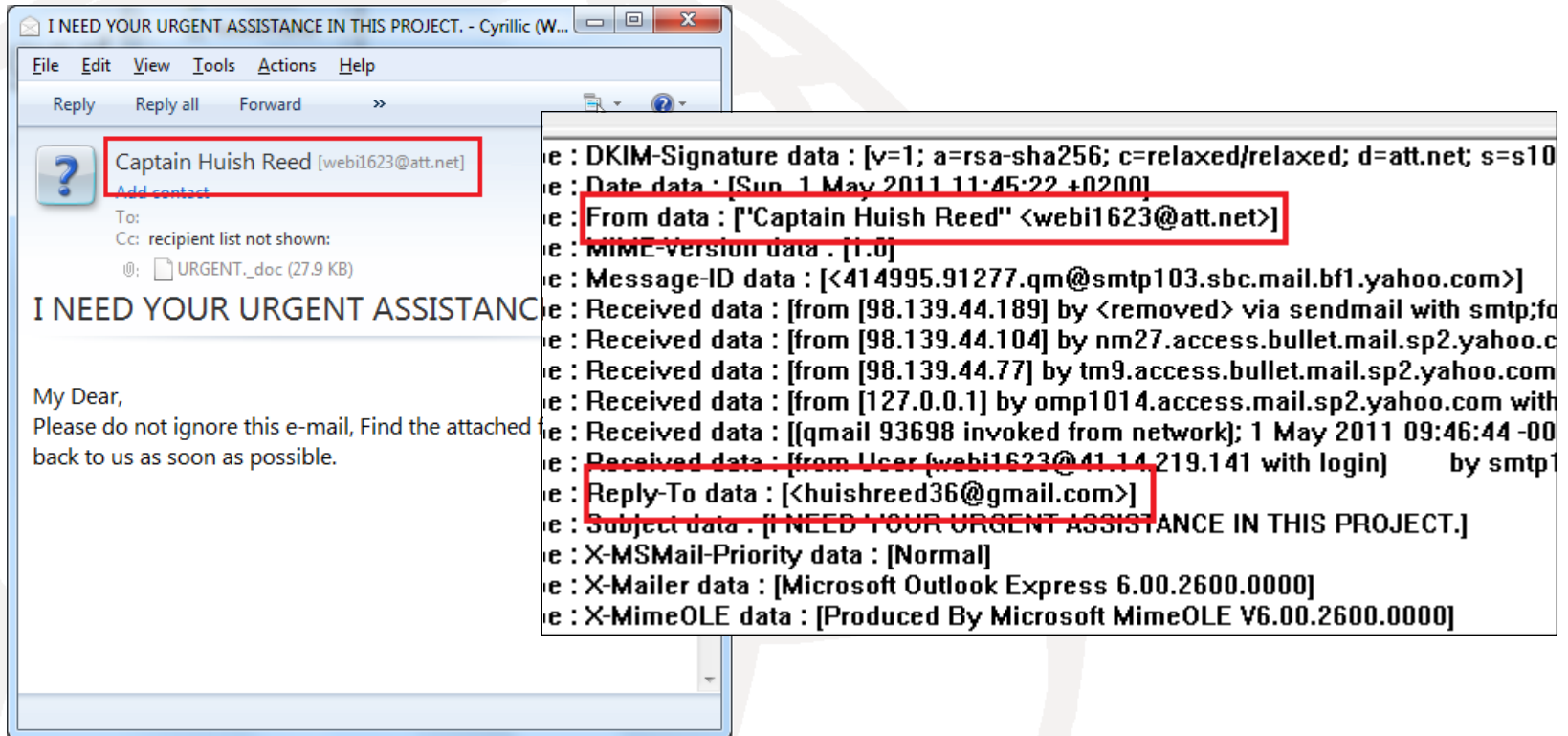
SPAM TRENDS AND TECHNIQUES

"Invisible Ink"



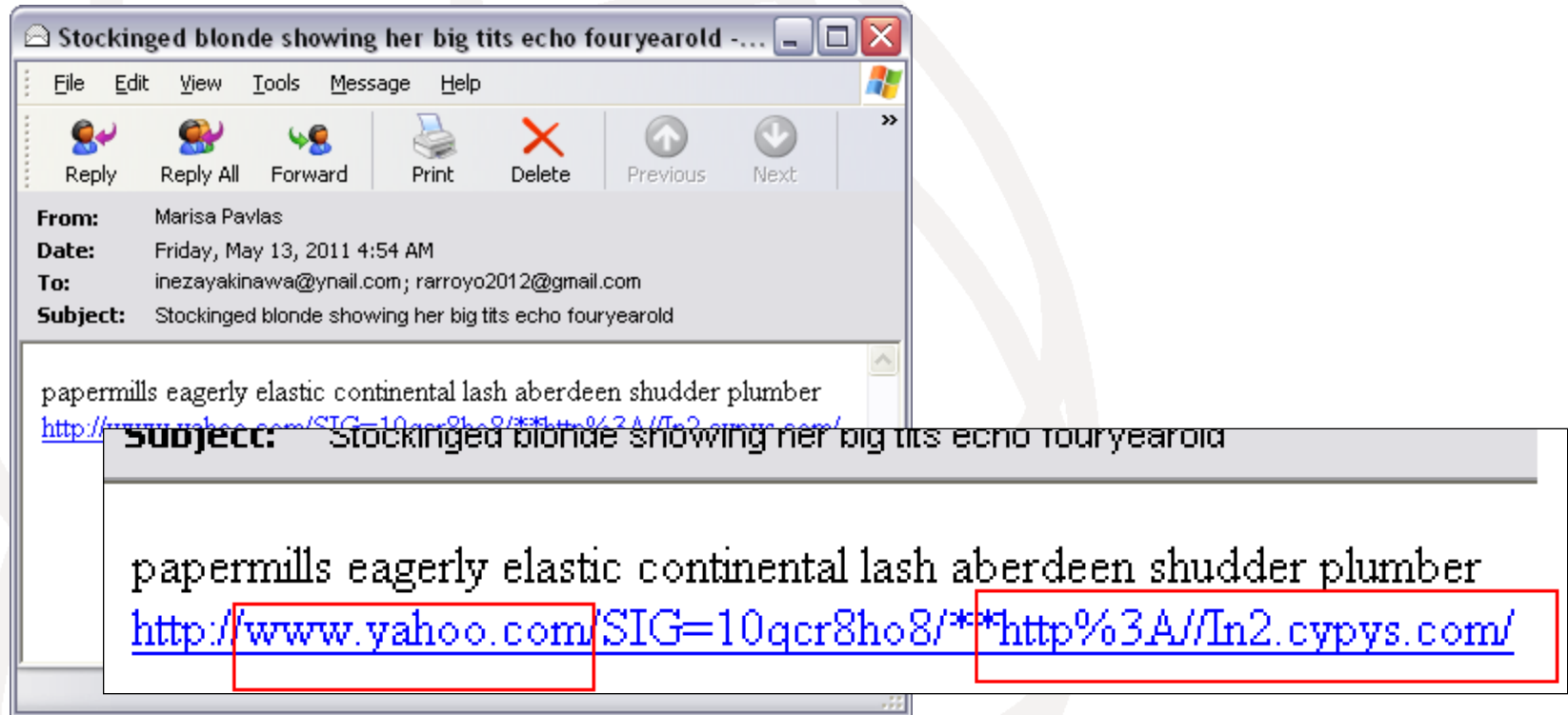
Concealment via HTTP formatting

Forging header info



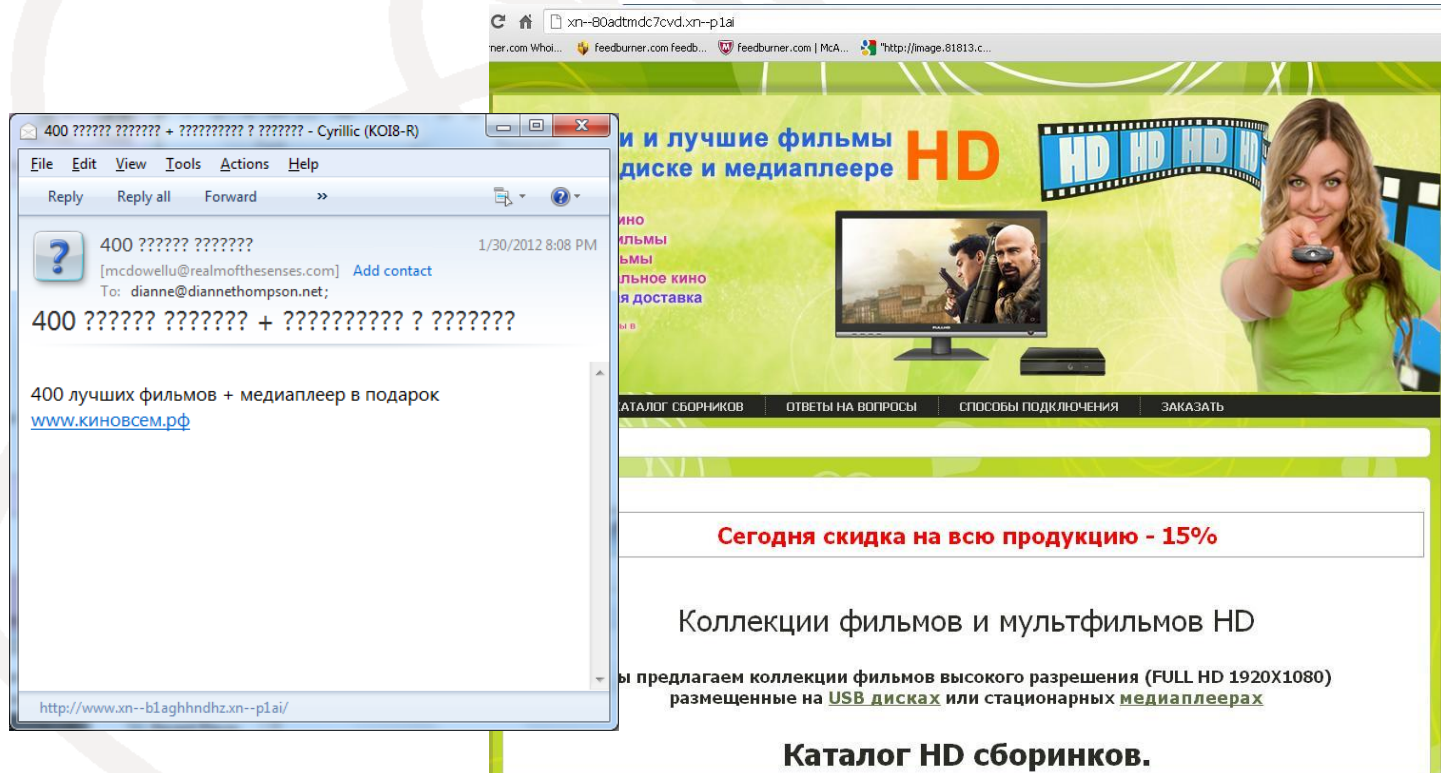
Adding fake header info to hide original source

URL redirection using popular sites



Inclusion of popular sites in links

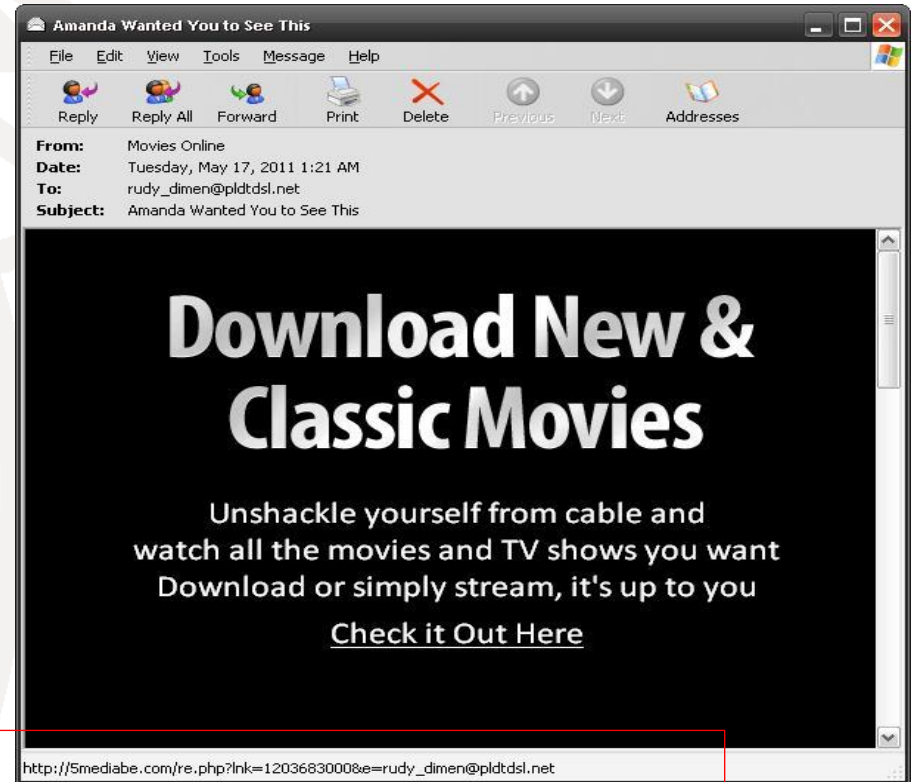
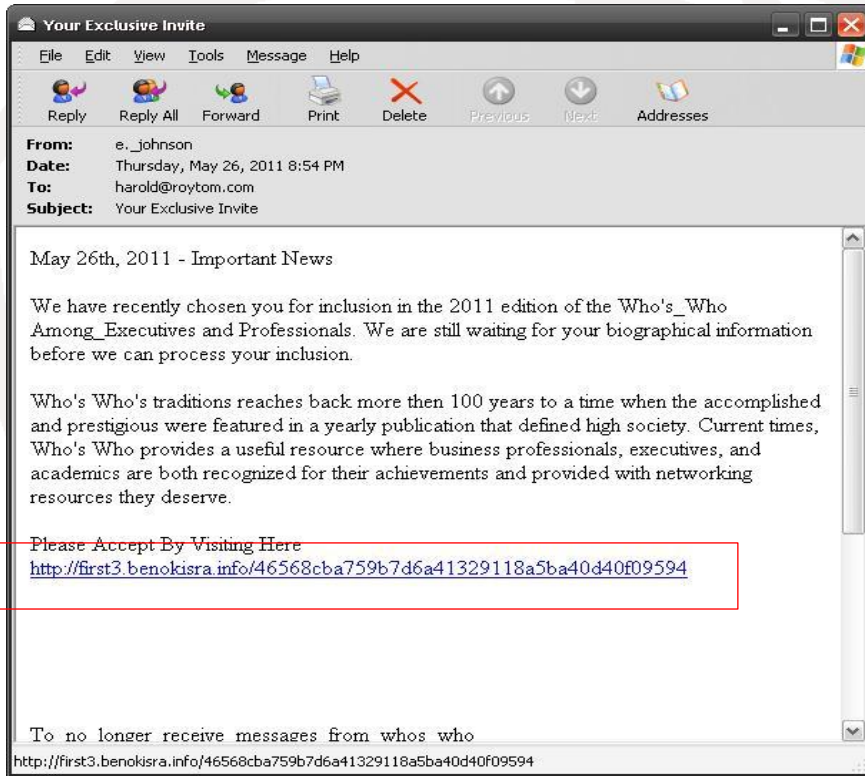
Obfuscating URLs ("Punycode" URLs)



The image shows a screenshot of an email client window and a web browser window. The email client window, titled "400 ?????? ?????? + ?????????? ? ???????? - Cyrillic (KOI8-R)", displays an email from "400 ?????? ??????" to "dianne@diannethompson.net". The email body contains the punycode URL "http://www.xn--b1aghhndhz.xn--p1ai/". The web browser window shows a website with a green and yellow theme, featuring a woman pointing a remote control. The website text includes "и лучшие фильмы HD", "Сегодня скидка на всю продукцию - 15%", and "Коллекции фильмов и мультфильмов HD".

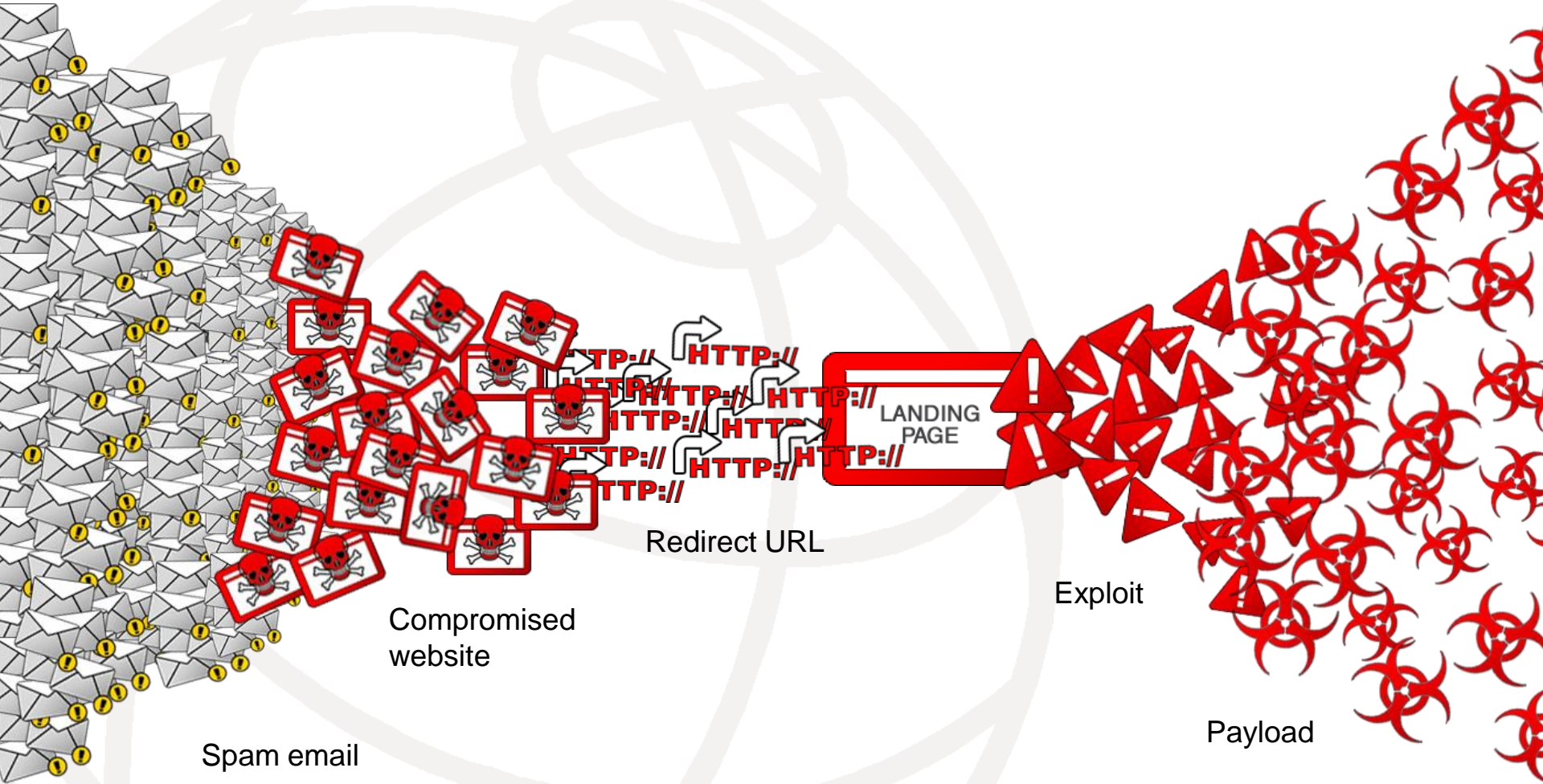
Converting Unicode characters to ASCII characters

Web bugs

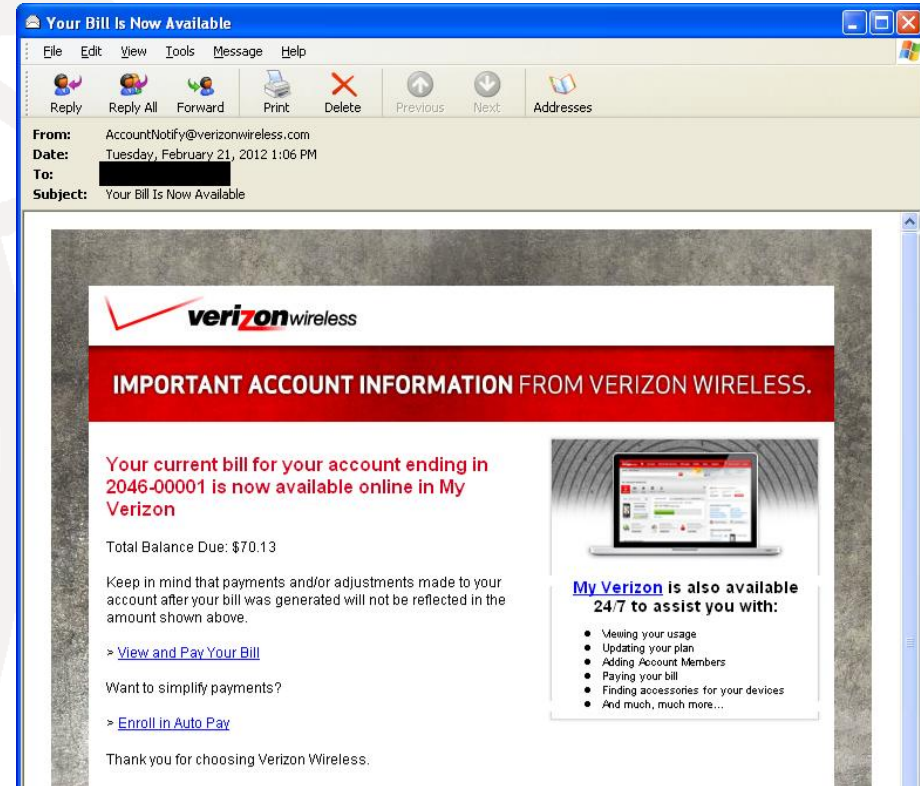
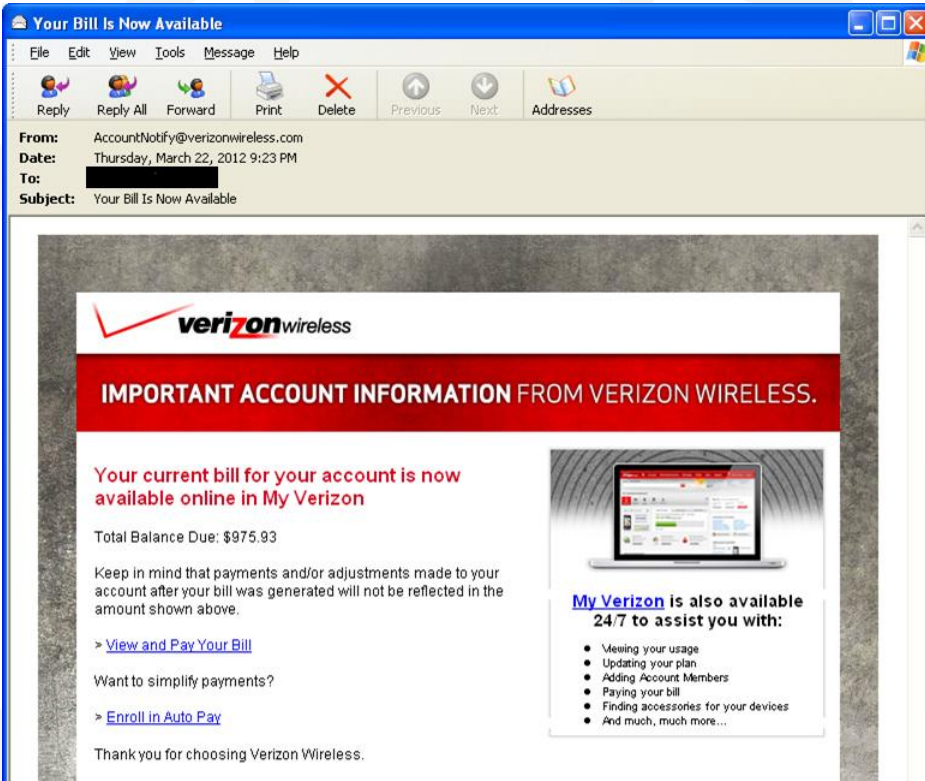


Tracking IDs to check active addresses

Blackhole Exploit Kit



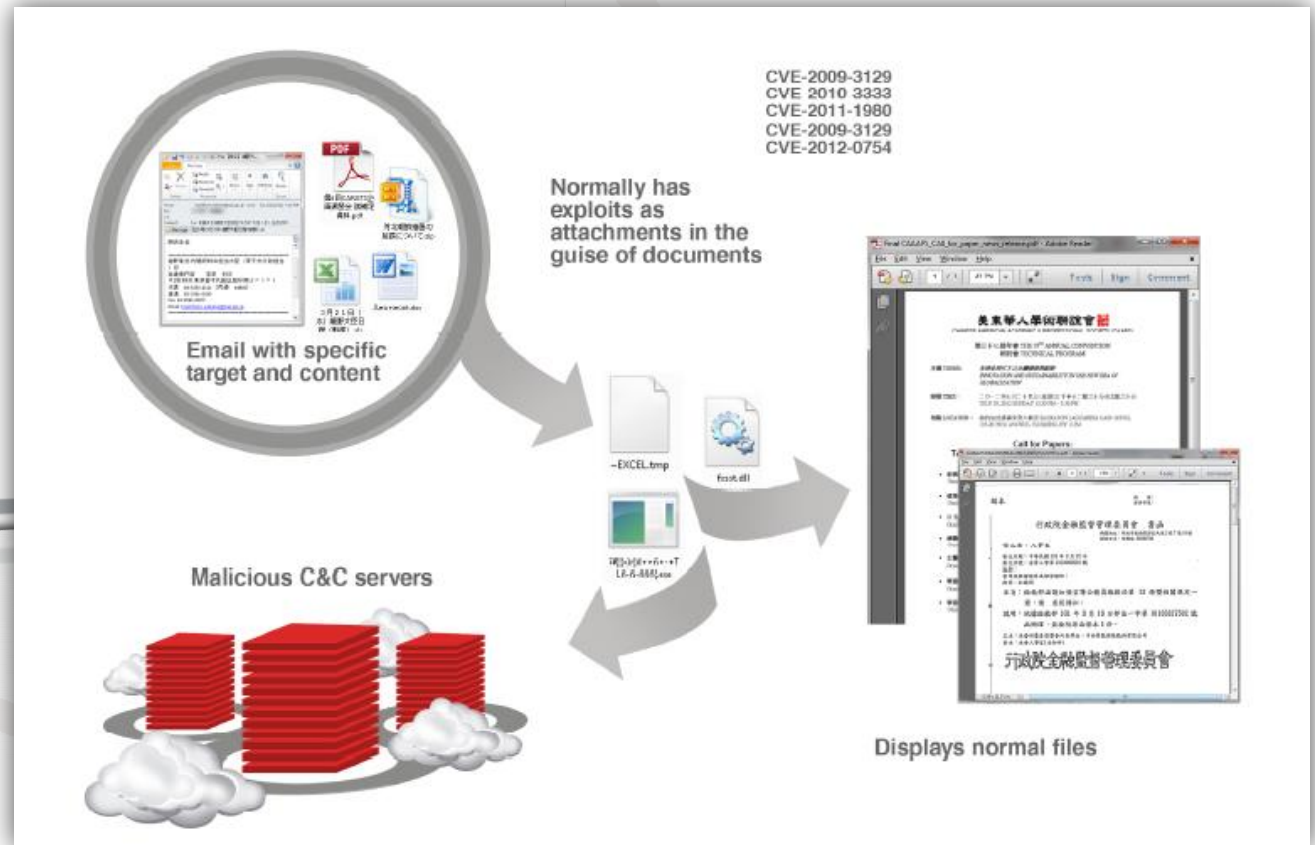
Real or Not Real?



Phish: <http://moriahfoundation.org/DRk5XAM2/index.html>

Legit: <https://nbillpay.verizonwireless.com/vzw/accountholder/mybill/BillingSummary.action>

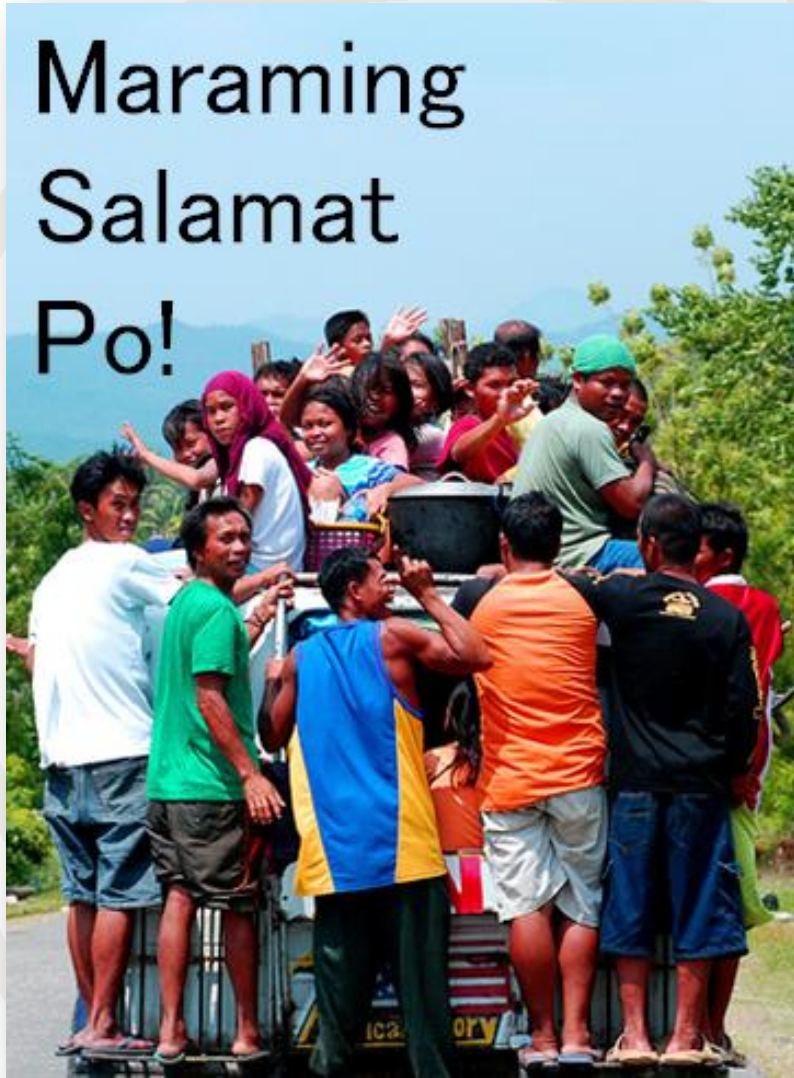
Spear-phishing email: most favored APT attack bait



Conclusion

- The number of spam will continue to decrease as solutions become “basic”
- The number of traditional spam will decrease as new vectors emerge
- Threat actors will design highly targeted attacks using customized spam
- Spam will still be “sexy” for cybercriminals

Maraming
Salamat
Po!



Philippines

