



New Techniques of Email-based Threats

Lalaine Gregorio | Dionisio Garcia
Trend Micro Email Reputation Services
September 2014



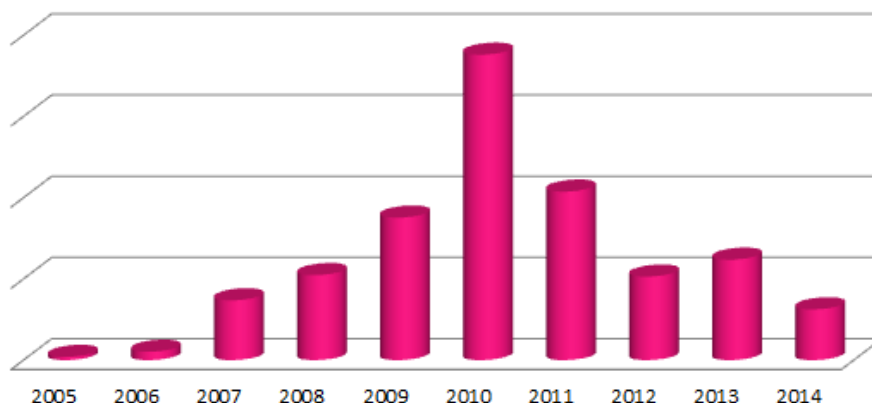
Brief History of Spam



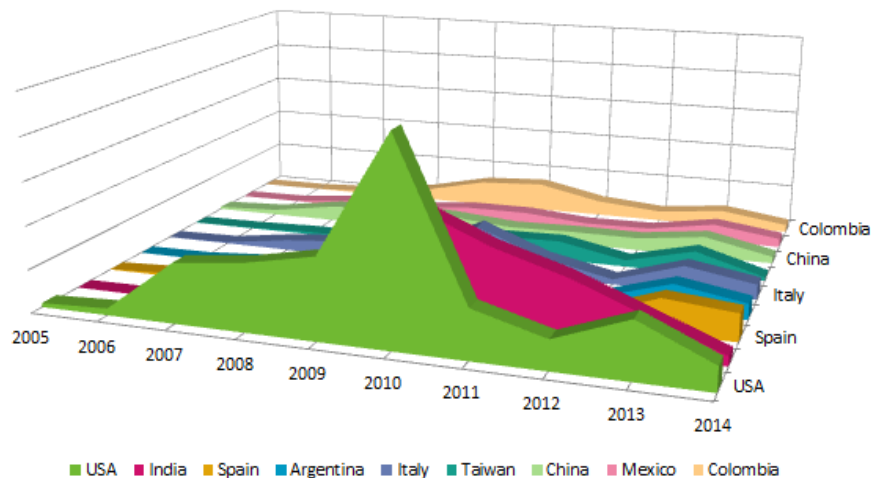
Historical Spam Volume

~50% decrease
in the overall
spam volume
since 2010

Historical Spam Volume



Historical Top Spam Sending Countries



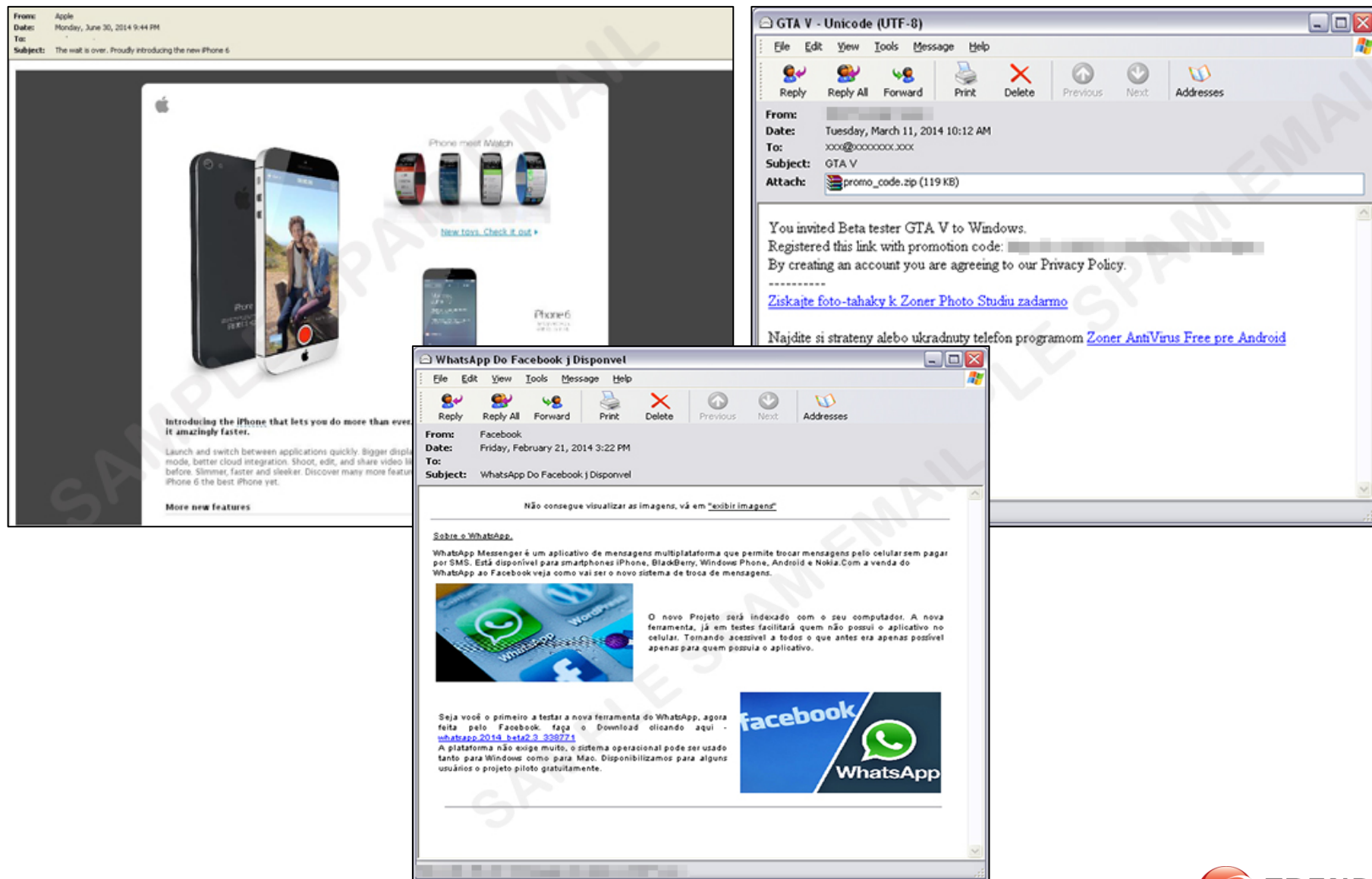
USA top spam
sending country

Spam 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

New Techniques of Email-based Threats

Newsworthy Spam used in Social Engineering Attack



Blackhole Exploit Kit Spam Run

Started to be active on **2012** using different legitimate company's email template

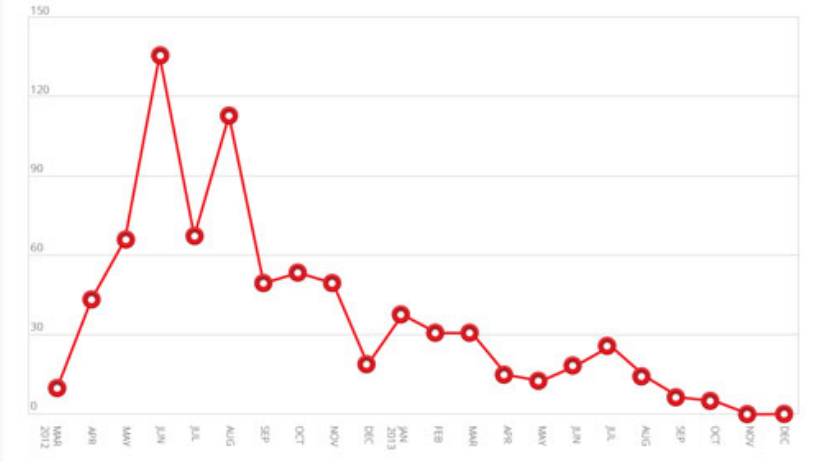


Figure 2. Number of BHEK campaigns from March 2012 to December 2013

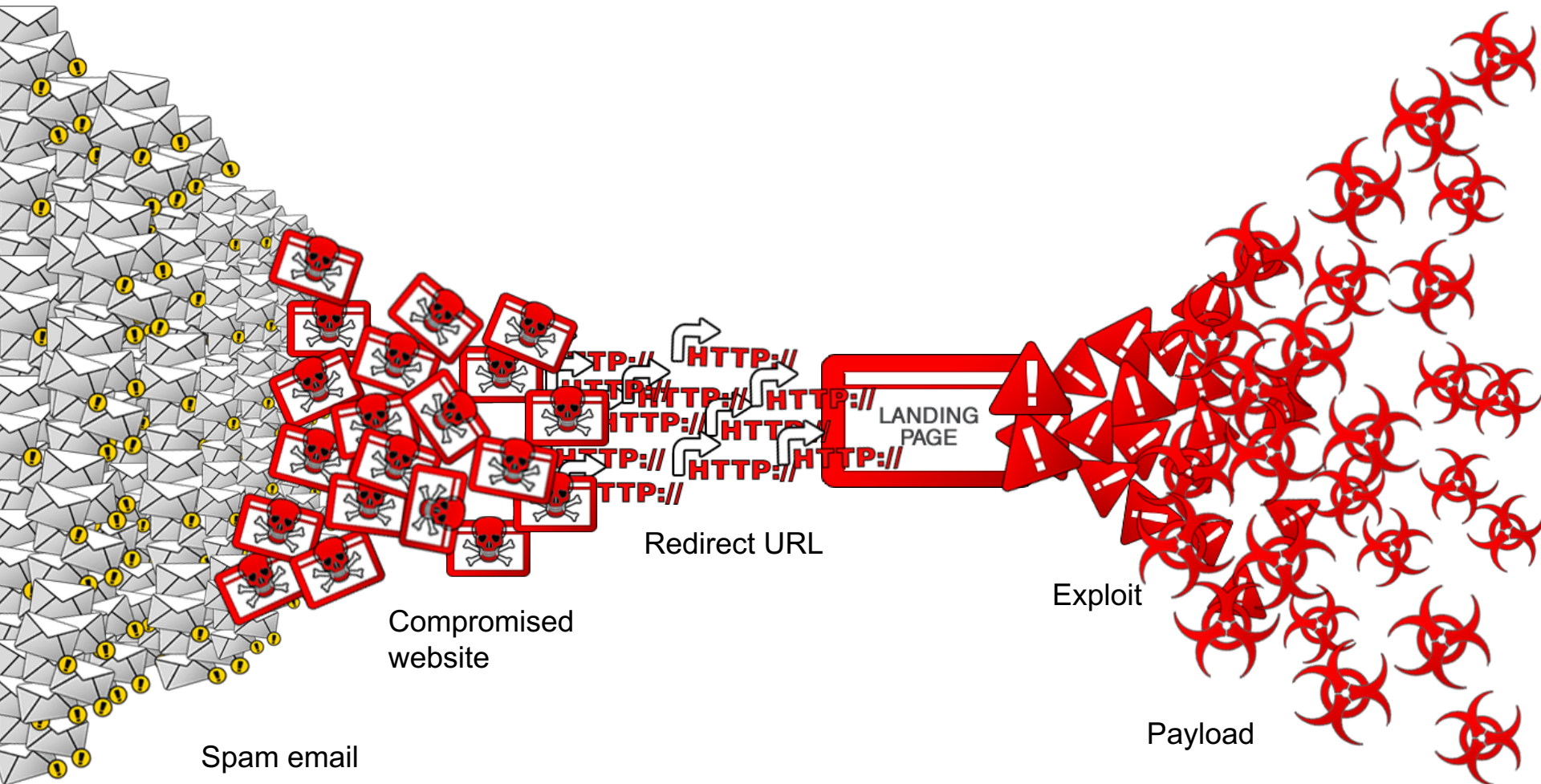
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
15 September	16	17	18	19	20	21
22	23	24 FDIC, NACHA	25 LinkedIn	26 Fax report	27 LinkedIn	28
29	30 IRS	1 October American Express	2 Pinterest	3 Stamps.com	4 LinkedIn, Dropbox	5 Facebook
6 PAUNCH ARRESTED	7	8	9	10	11	12
13	14	15	16	17	18	19

Table 1. BHEK spam campaigns identified

BHEK campaign lasts for more or less **2 years**

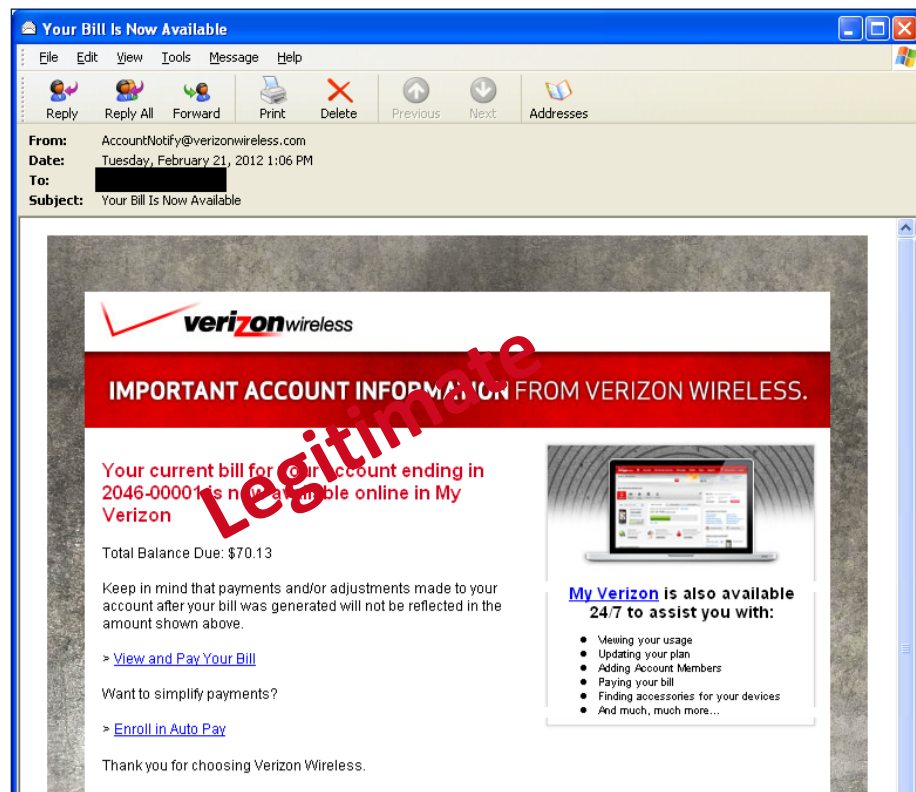
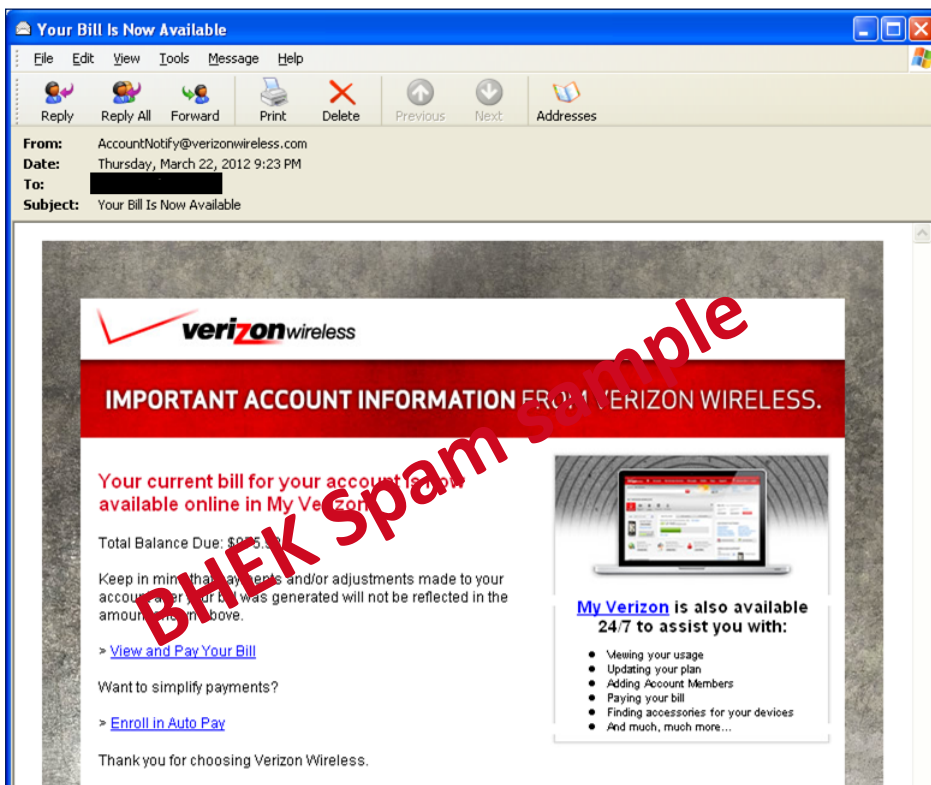
Source : <http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/>
<http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-arrests-how-has-the-underground-reacted/>

Blackhole Exploit Kit



Blackhole Exploit Kit Infection Chain

Legitimate vs. BHEK Spam Sample



Phish:

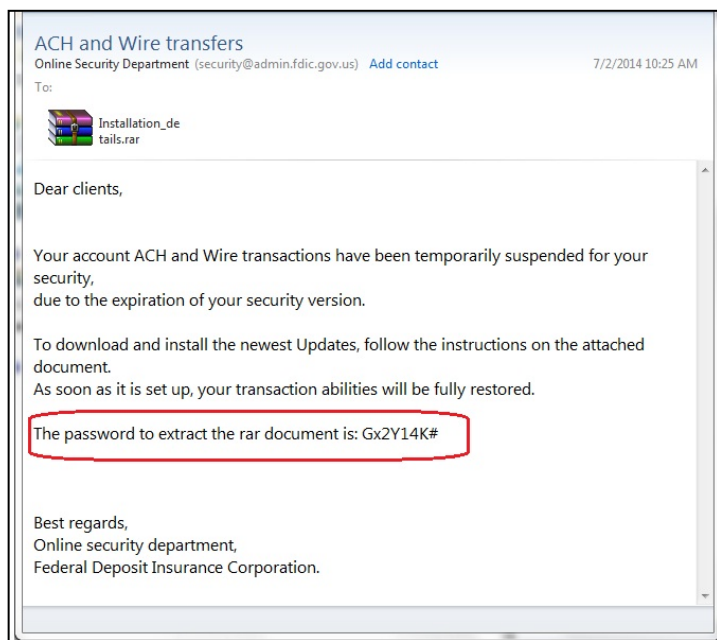
<http://moriahfoundation.org/DRk5XAM2/index.html>

Legit:

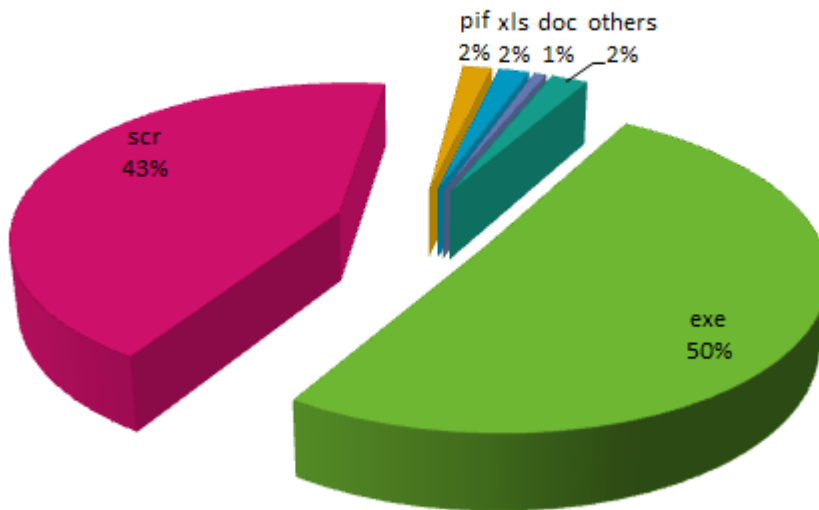
<https://nbillpay.verizonwireless.com/vzw/accountholder/mybill/BillingSummary.action>

MalSpam With Malicious Attachment

- Similar to BHEK campaign it uses different spam templates using legitimate companies to lure its victim
- Some spam uses password protected executable malware files to make it more legitimate
- Majority of the MalSpam campaign is in .exe format mostly in a compressed file

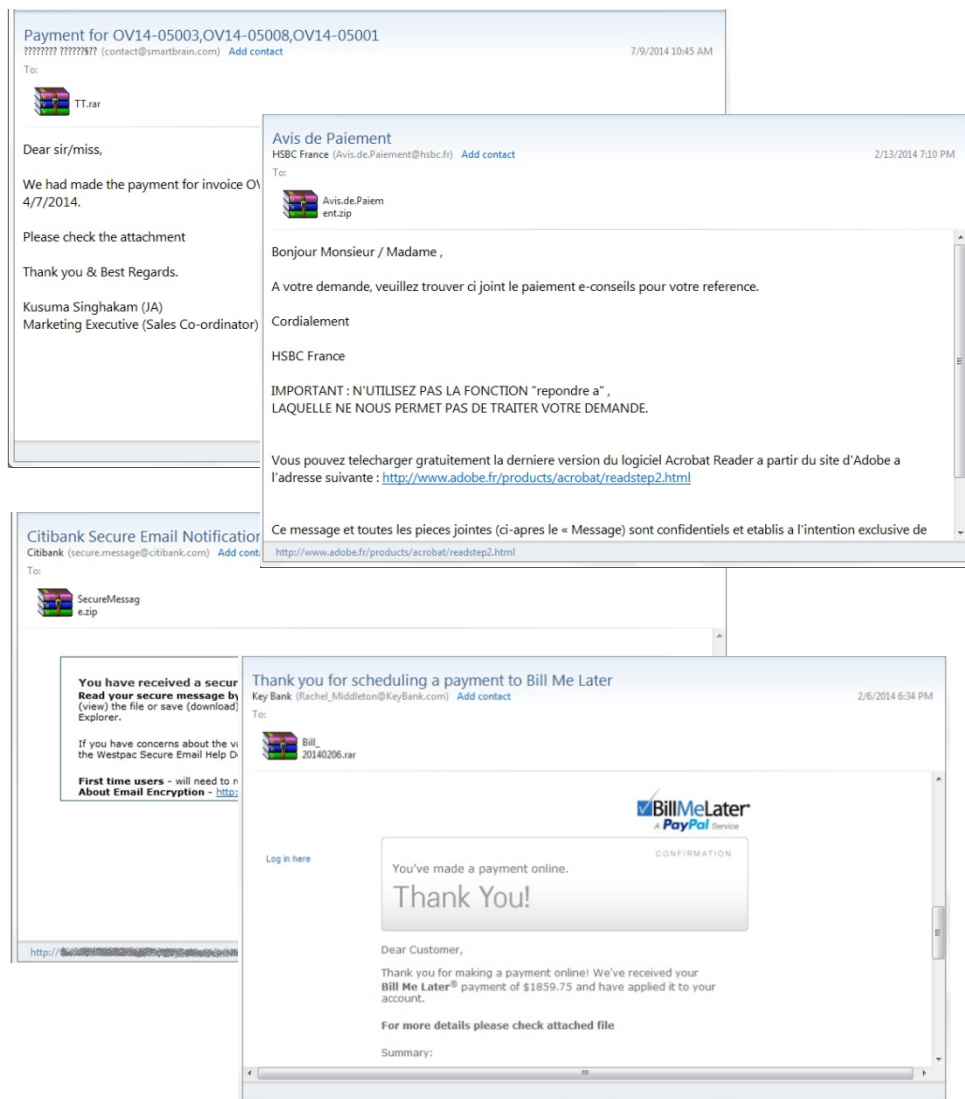


Top MalSpam Attachment Type

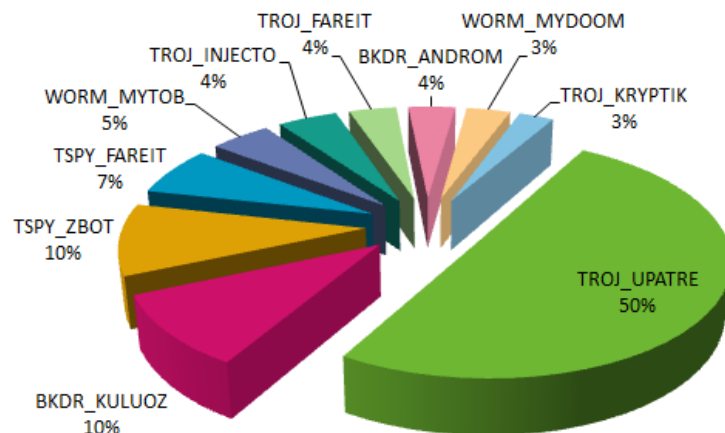


MalSpam With Malicious Attachment

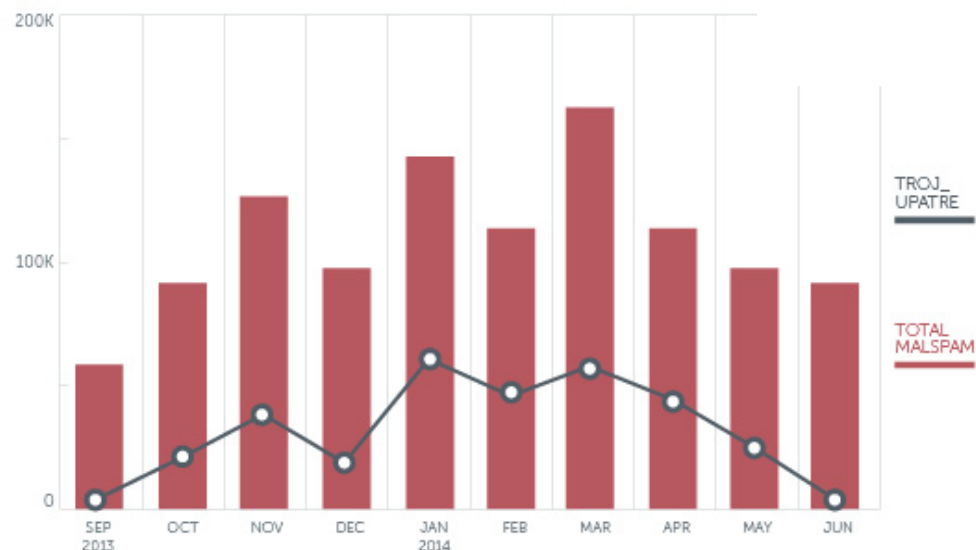
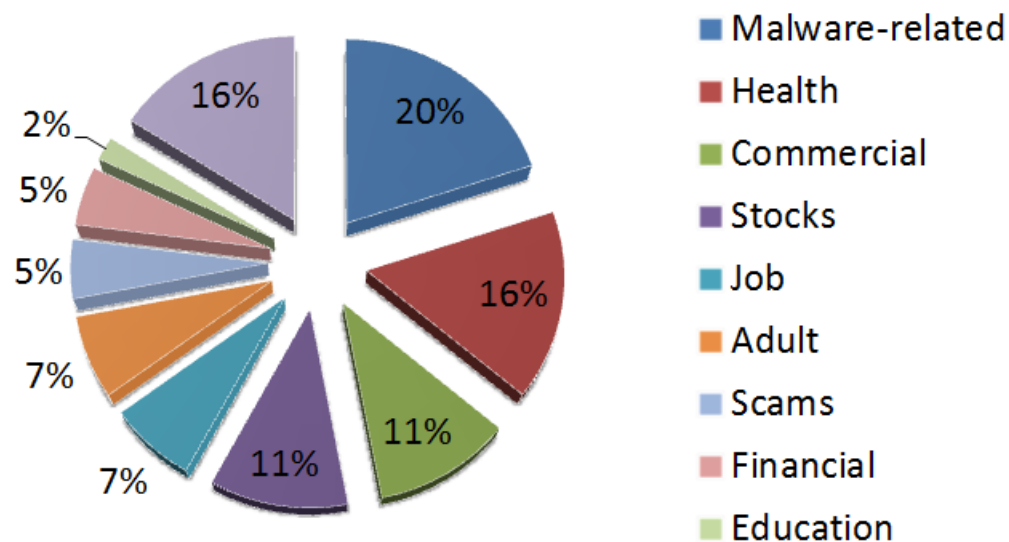
~50% of MalSpam sample carries TROJ_UPATRE variant



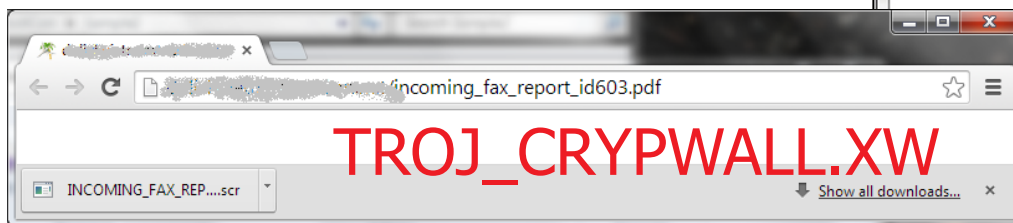
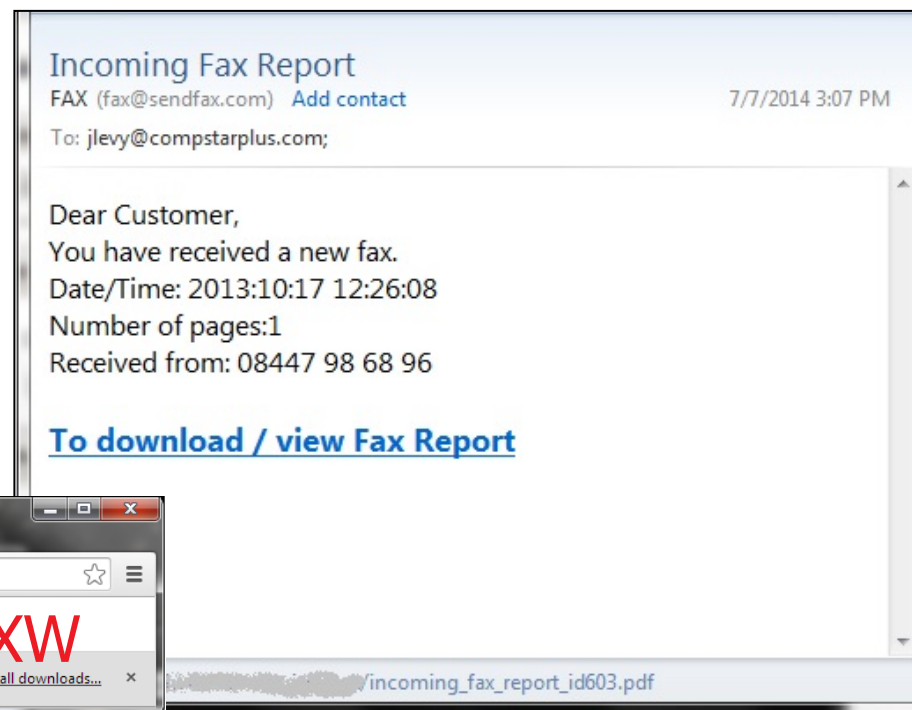
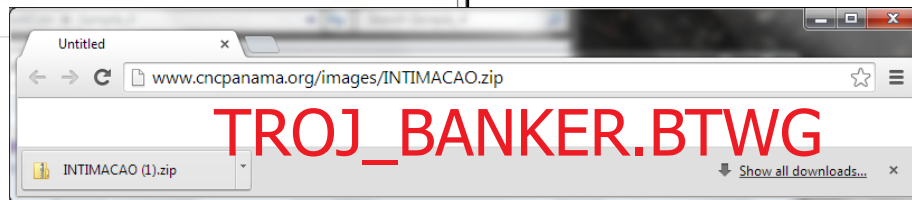
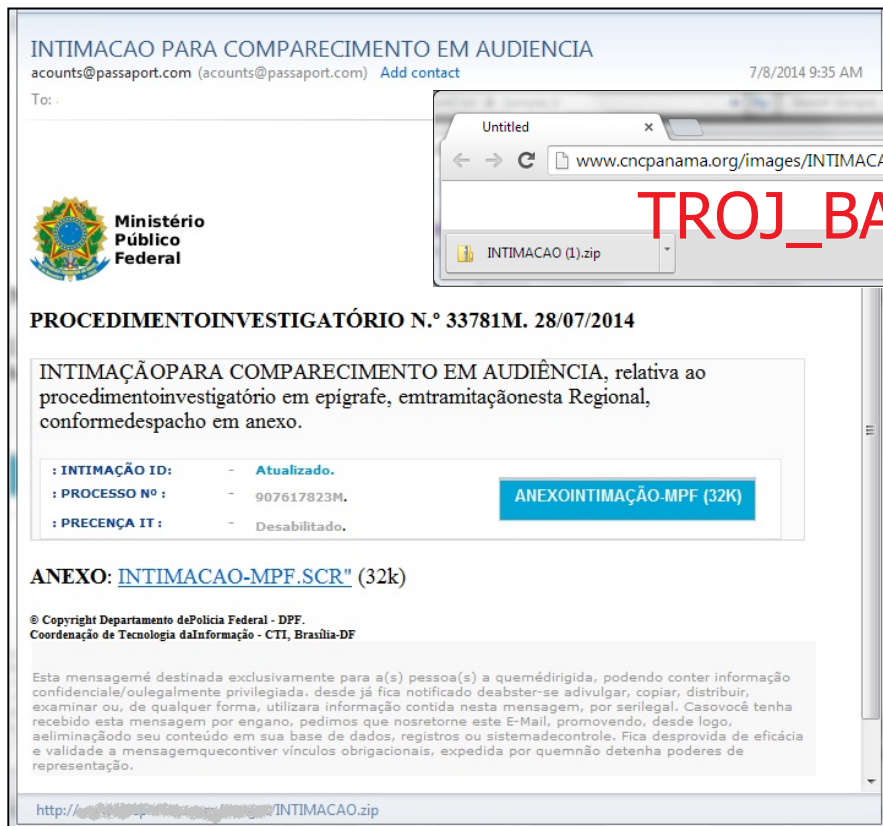
2014 Top Malware from Spam



1H – 2014 Top Spam Categories



MalSpam with Malicious URL



Popular Cloud Services used in MalSpam Campaign

From: Incoming Fax <no-reply@efax.co.uk> **Sent:** Thu 5/29/2014 5:37 AM
To: [Redacted]
Cc: [Redacted]
Subject: INCOMING FAX REPORT: Remote ID: 896-576-6945

INCOMING FAX REPORT

Date/Time: Thu, 29 May 2014 11:37:02 +0100
Speed: 4096bps
Connection time: 00:04
Pages: 3
Resolution: Normal
Remote ID: 859-835-4409
Line number: 8
DTMF/DID:
Description: Internal report

We have uploaded fax report file:

[Redacted]

From: Payroll Invoice <payroll@intuit.com>
To: [Redacted]
Cc: [Redacted]
Subject: Payment Overdue - Please respond

We have uploaded previous month reports on dropbox. Please download your file:

[Redacted]

Sincerely,
Marissa Bradley

This e-mail has been sent from an automated system.

CONFIDENTIAL NOTICE: The contents of this message, including any attachments, are confidential and are intended solely for the use of the person or entity to whom the message was addressed. If you are not the intended recipient of this message, please be advised that any dissemination, distribution, or use of the contents of this message is strictly prohibited. If you received this message in error, please notify the sender. Please also permanently delete all copies of the original message and any attached documentation. Thank you.

Emissão Formulario de Regularização
Ana Paula (info@quitacao.com.br) [Add contact](#) 6/30/2014 8:25 PM
To:

Advogados Associados - LC MARCON,

Prezado Cliente(a),

Tentamos entrar em contato com o Senhor(a) pelo telefone mais não obtemos êxito para não fosse incluso no sistema de proteção ao crédito.

Por este motivo estamos mantendo contato via e-mail para regularização de seu débito, p... validade até a data 03.07.2014.

Segue em anexo o documento para regularização e sua Nota Fiscal de gastos.

Sua Nota Fiscal de gastos, [N&F ID.0031006](#) (60KB).

Documento De Regularização, [DocumentoDeRegularização.pdf](#) (134KB).

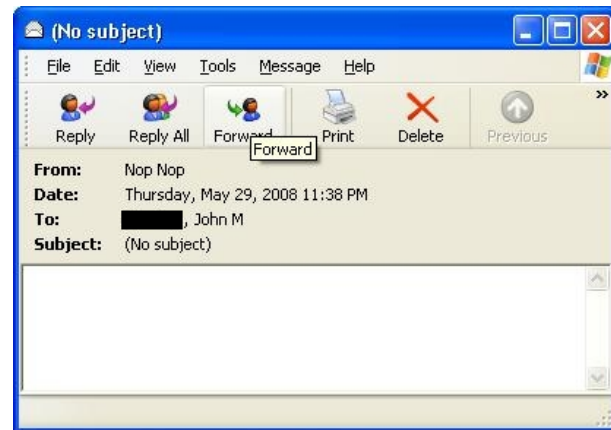
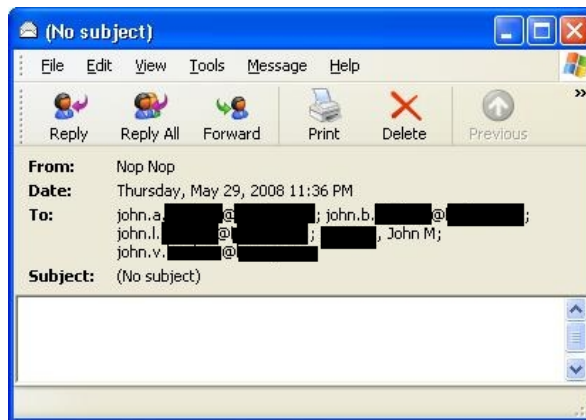
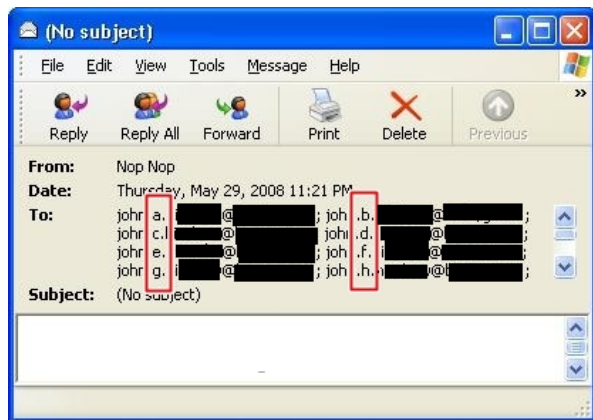
Caso não consiga contendo um novo documento.

Advogados e Associados
LC Marcon.

<https://docs.google.com/...>

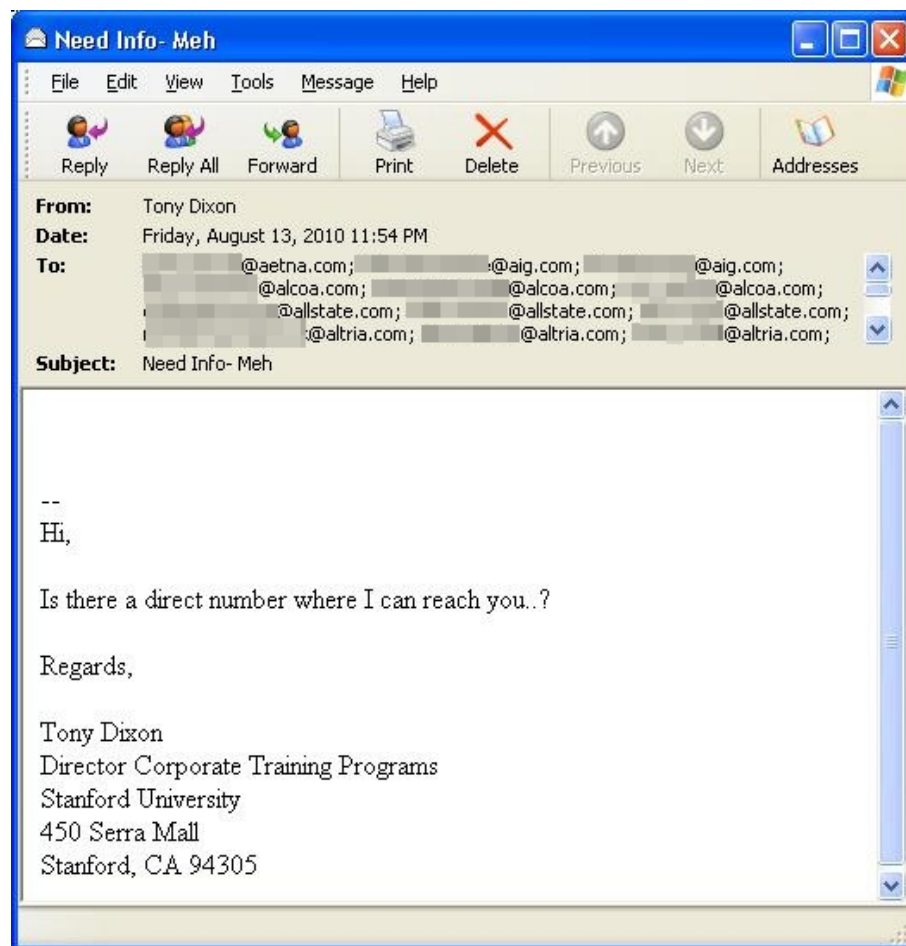
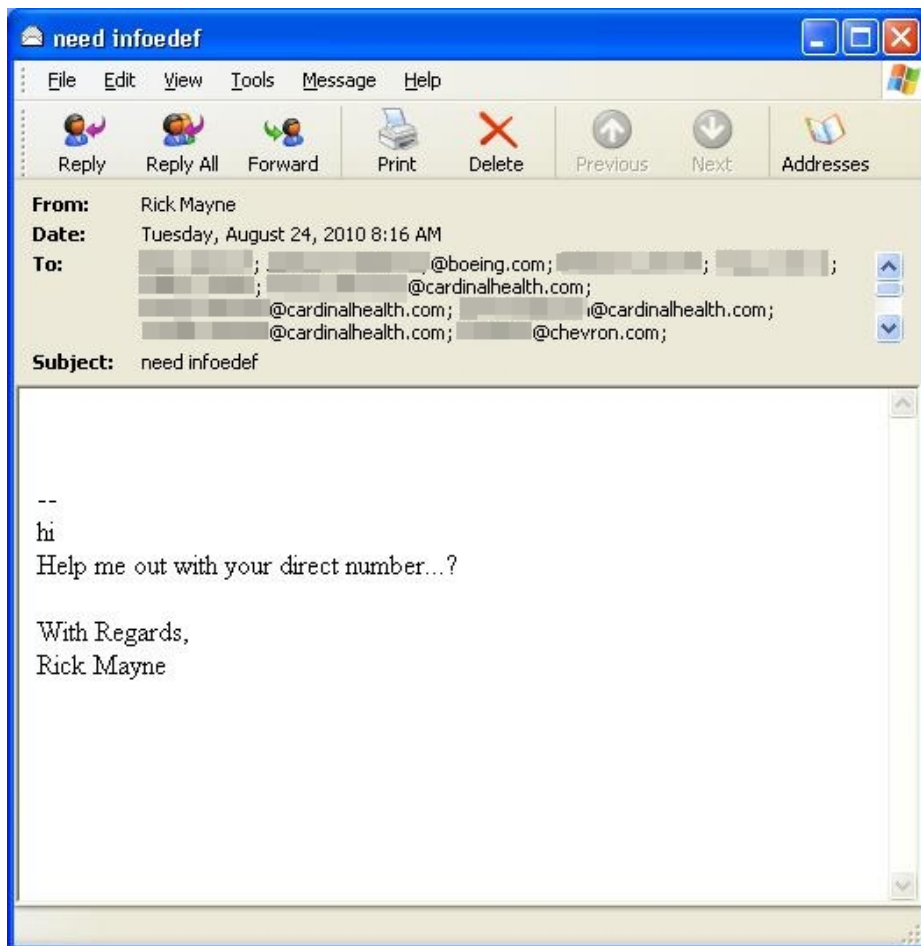
Nota Fiscal ID.0041007.zip - ZIP archive, unpacked size 375,29
Name
..
Nota Fiscal ID.0041007.cpl
TROJ_BANLOAD.YAA
Total 375,296 bytes in 1 file

Directory Harvest Attack

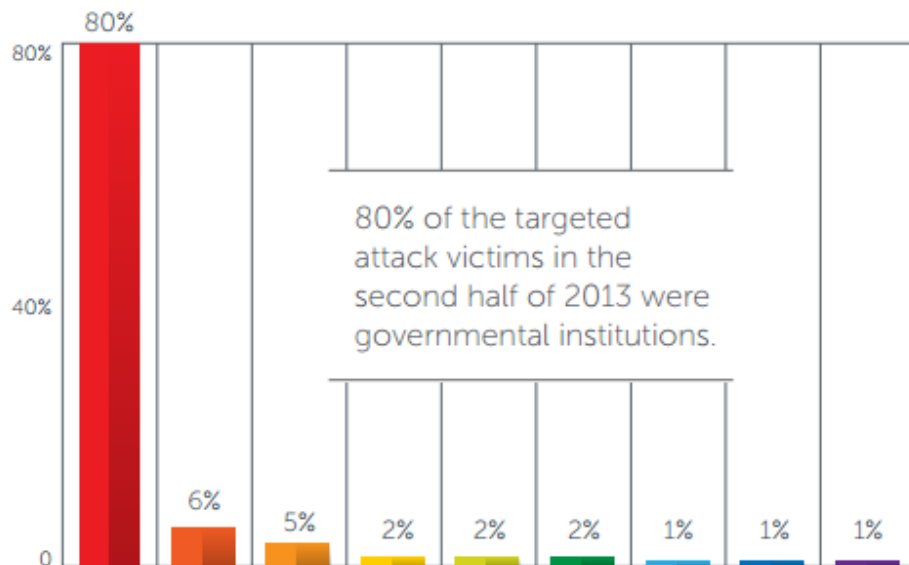


Spam	Timestamp	From	To	Recipients
#1	5/29/08 8:21:04	nopnop32@yahoo.com	john.a.<removed>@<removed>.com - john.z.<removed>@<removed>.com	26
#2	5/29/08 8:36:36	nopnop32@yahoo.com	john.a.<removed>@<removed>.com john.b.<removed>@<removed>.com john.l.<removed>@<removed>.com john.m.<removed>@<removed>.com john.v.<removed>@<removed>.com	5
#3	5/29/08 8:38:58	nopnop32@yahoo.com	john.m.<removed>@.<removed>.com	1

Spear Phishing Campaign in 2010



Targeted Attack



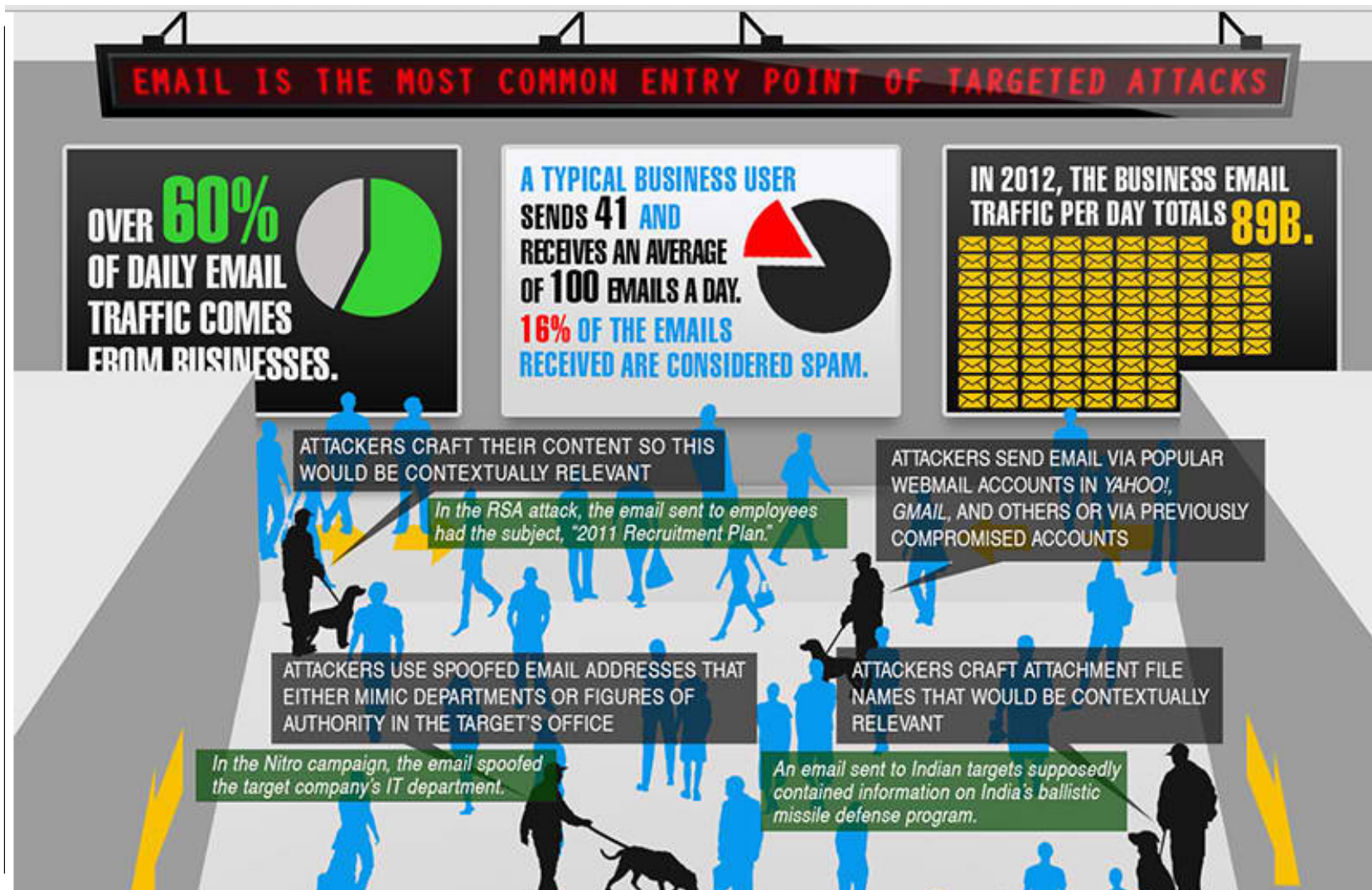
Targeted attacks seen by industry

- Government
- IT
- Financial services
- Education
- Industrial
- Telecommunications
- Consumer electronics
- Aerospace
- Aviation



Source: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/2H_2013_Targeted_Attack_Campaign_Report.pdf

Infographic | Email's Role in APT Campaigns



Source : <http://about-threats.trendmicro.com/us/infographics/infograph/covert-arrivals-emails-role-in-apt-campaigns>

Best Practices

Email Best Practices



Be cautious on attachment that came from suspicious source



Hovering your mouse pointer to the visible link



Check for the intent of the email, sometimes the content of spam are too good to be true



Contact the sender via phone or request for a personal meeting



Regularly get updates on your soft wares.



Leverage on all available products to protect yourself from different type of threats to have a safe exchange of digital information

References

- <http://about-threats.trendmicro.com/us/threatencyclopedia#spam>
- <http://blog.trendmicro.com/trendlabs-security-intelligence/category/spam/>
- <http://about-threats.trendmicro.com/us/infographics/>

Thank You!