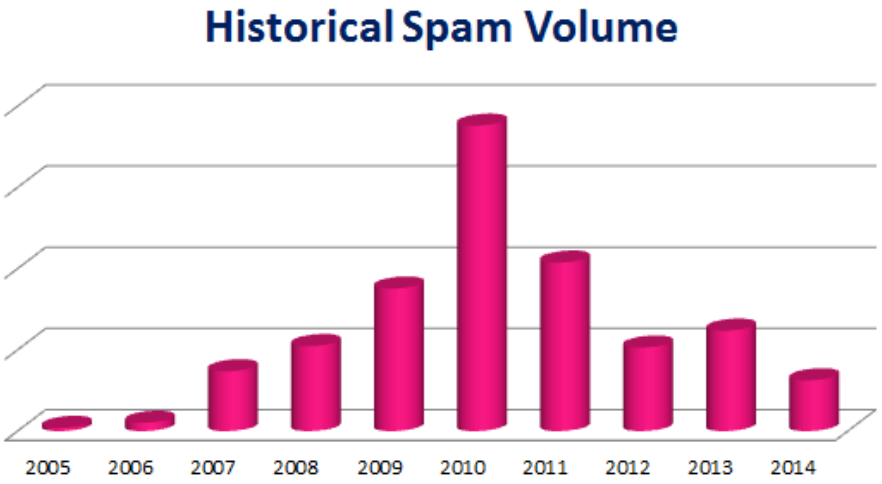
New Techniques of Email-based Threats

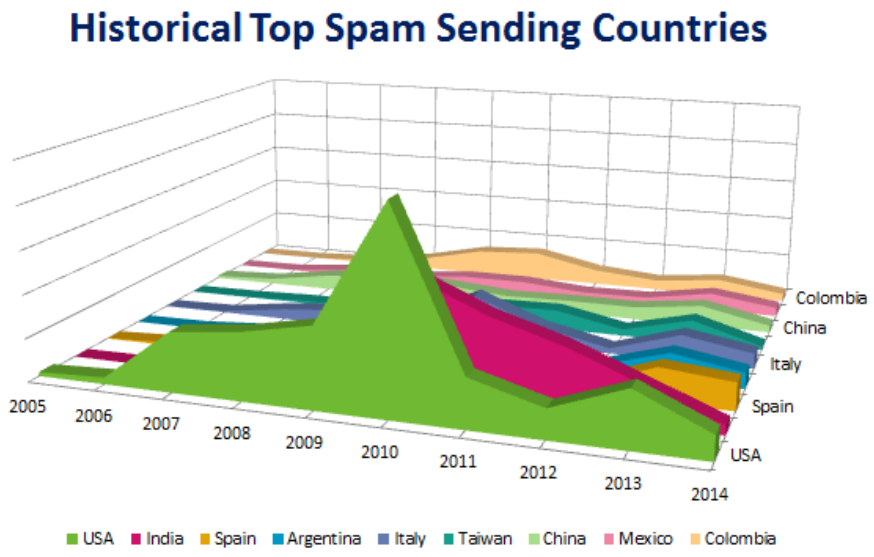
Lalaine Gregorio | Dionisio Garcia
Trend Micro Email Reputation Services
September 2014

Brief History of Spam

Historical Spam Volume

~50% decrease in the overall spam volume since 2010





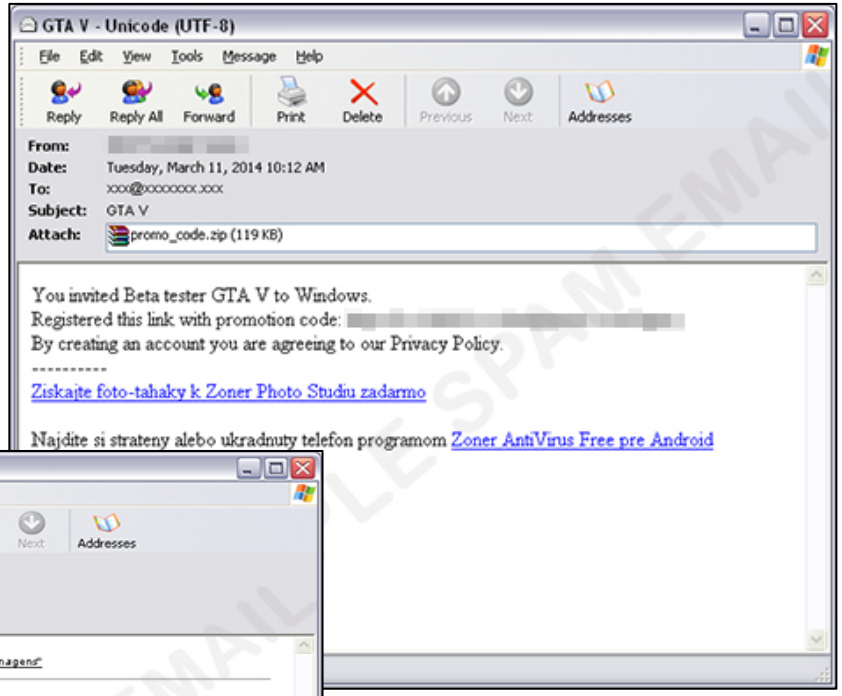
USA top spam sending country

Spam as a Service (SaaS)

OFFERING	PRICE
• Cheap email spamming service	US$10 pero 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

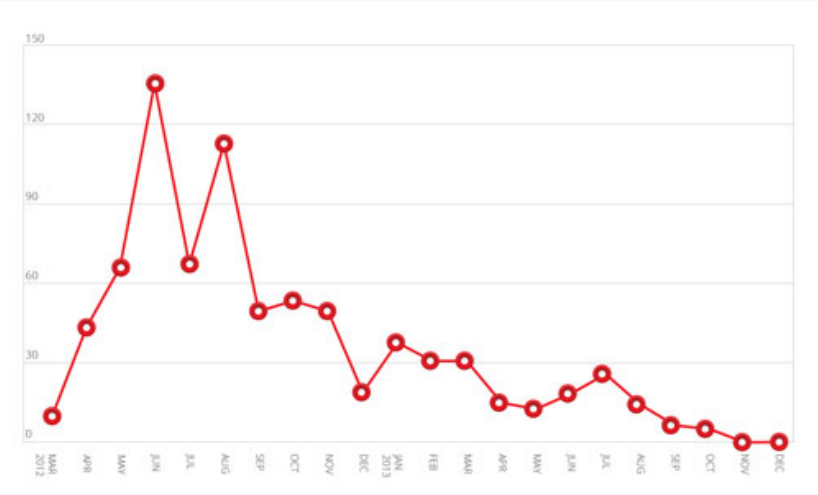


Figure 2. Number of BHEK campaigns from March 2012 to December 2013

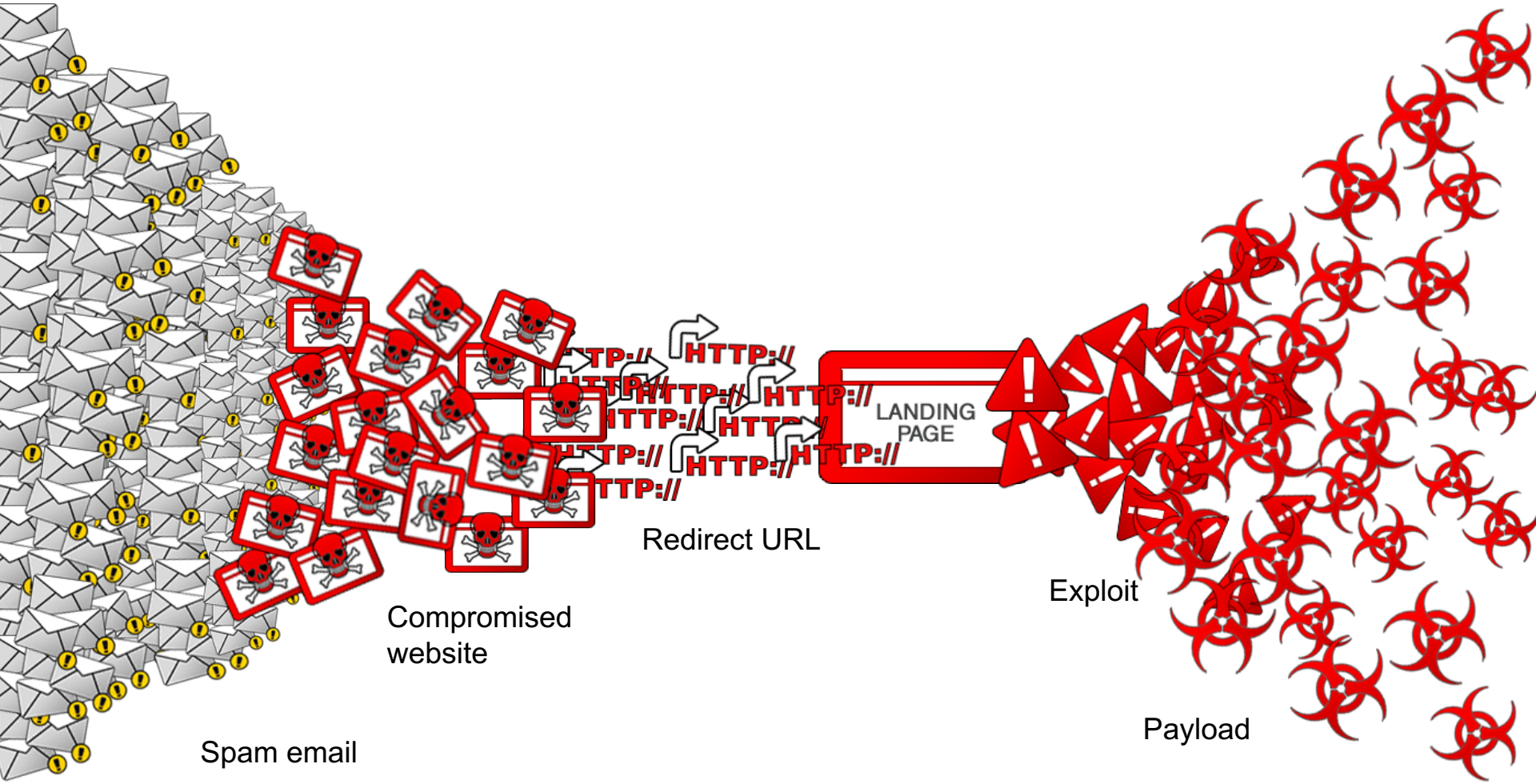
Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
15 *September*	16	17 FDIC, NACHA	18 LinkedIn	19 Fax report	20 LinkedIn	21
22	23	24	25	26	27 LinkedIn	28 Facebook
29	30 IRS	1 *October* American Express	2 Pinterest	3 Stamps.com	4 LinkedIn, Dropbox	5
6 PAUNCH ARRESTED	7	8	9	10	11	12
13	14	15	16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

Table 1. BHEK spam campaigns identified

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

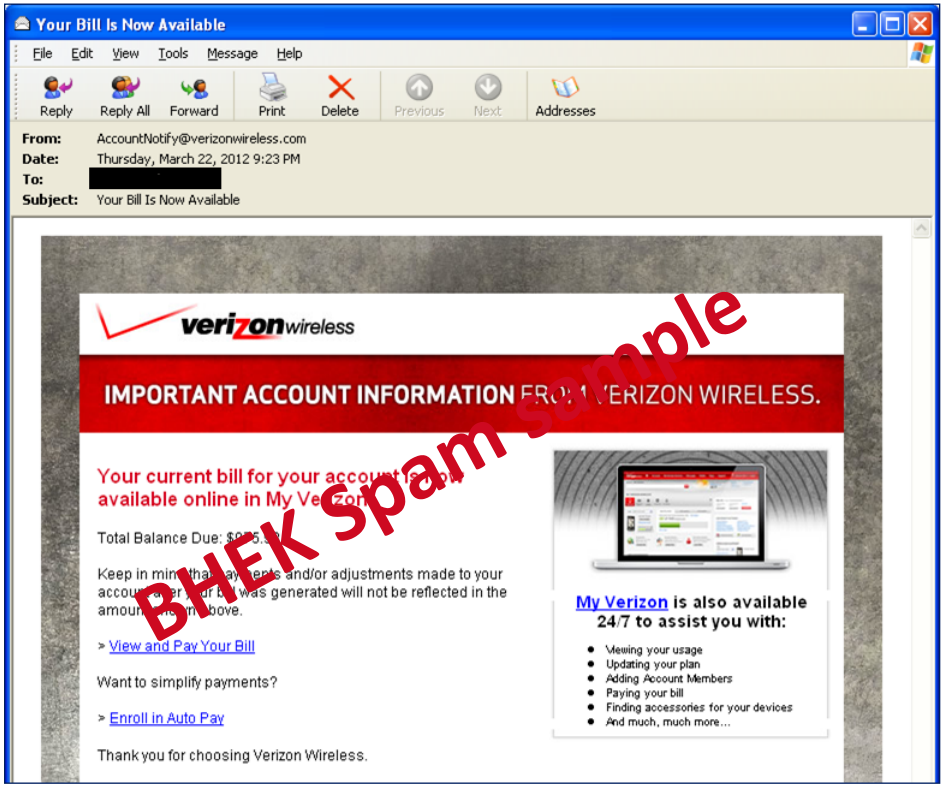
Source : http://blog.trendmicro.com/trendlabs-security-intelligence/a-year-of-spam-the-notable-trends-of-2013/
http://blog.trendmicro.com/trendlabs-security-intelligence/blackhole-arrests-how-has-the-underground-reacted/

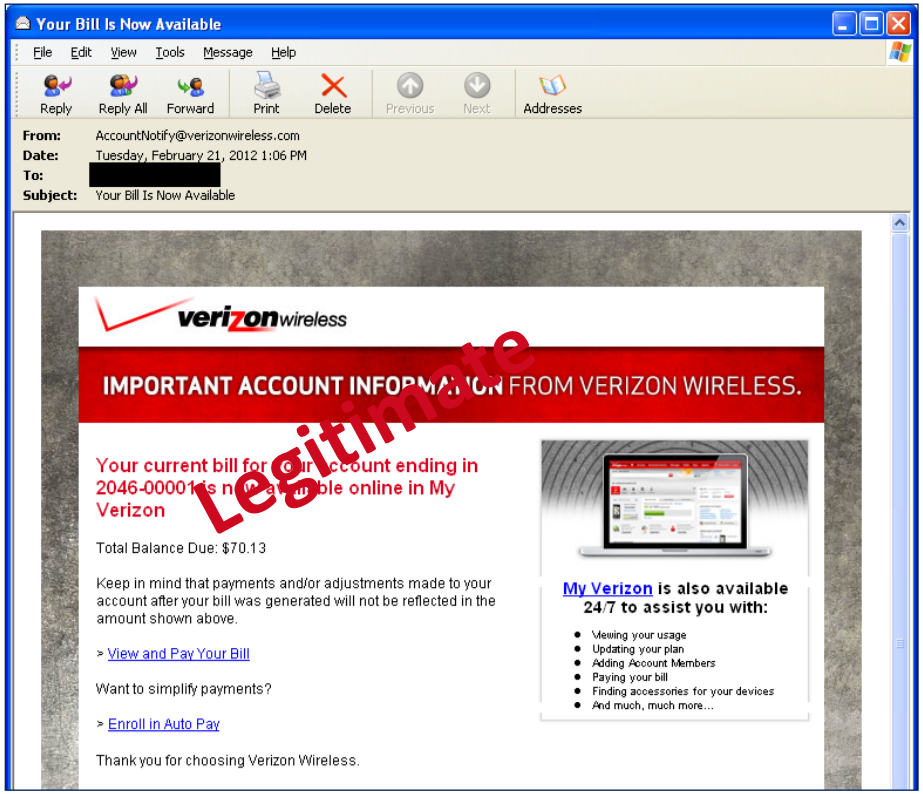
Blackhole Exploit Kit



Blackhole Exploit Kit Infection Chain

Legitimate vs. BHEK Spam Sample



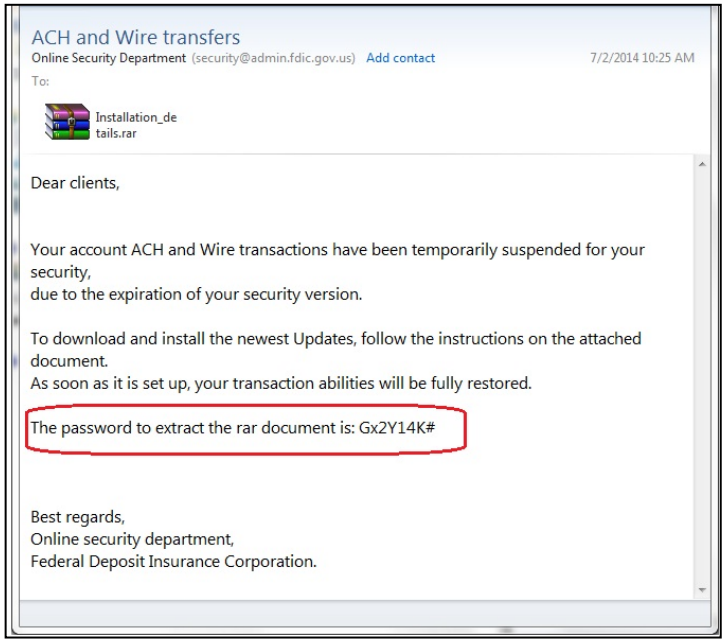


Phish: http://moriahfoundation.org/DRk5XAM2/index.html

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


ACH and Wire transfers

Online Security Department (security@admin.fdic.gov.us) Add contact 7/2/2014 10:25 AM

To:

Installation_details.rar

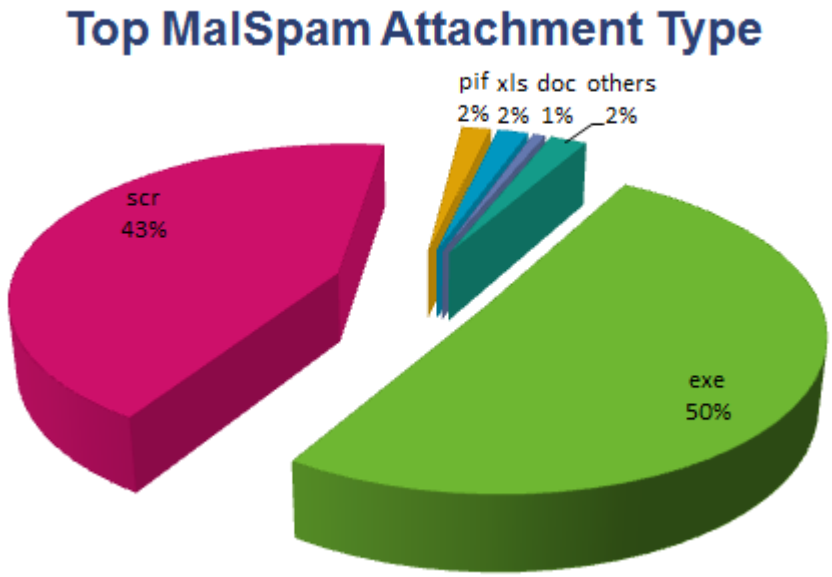
Dear clients,

Your account ACH and Wire transactions have been temporarily suspended for your security,
due to the expiration of your security version.

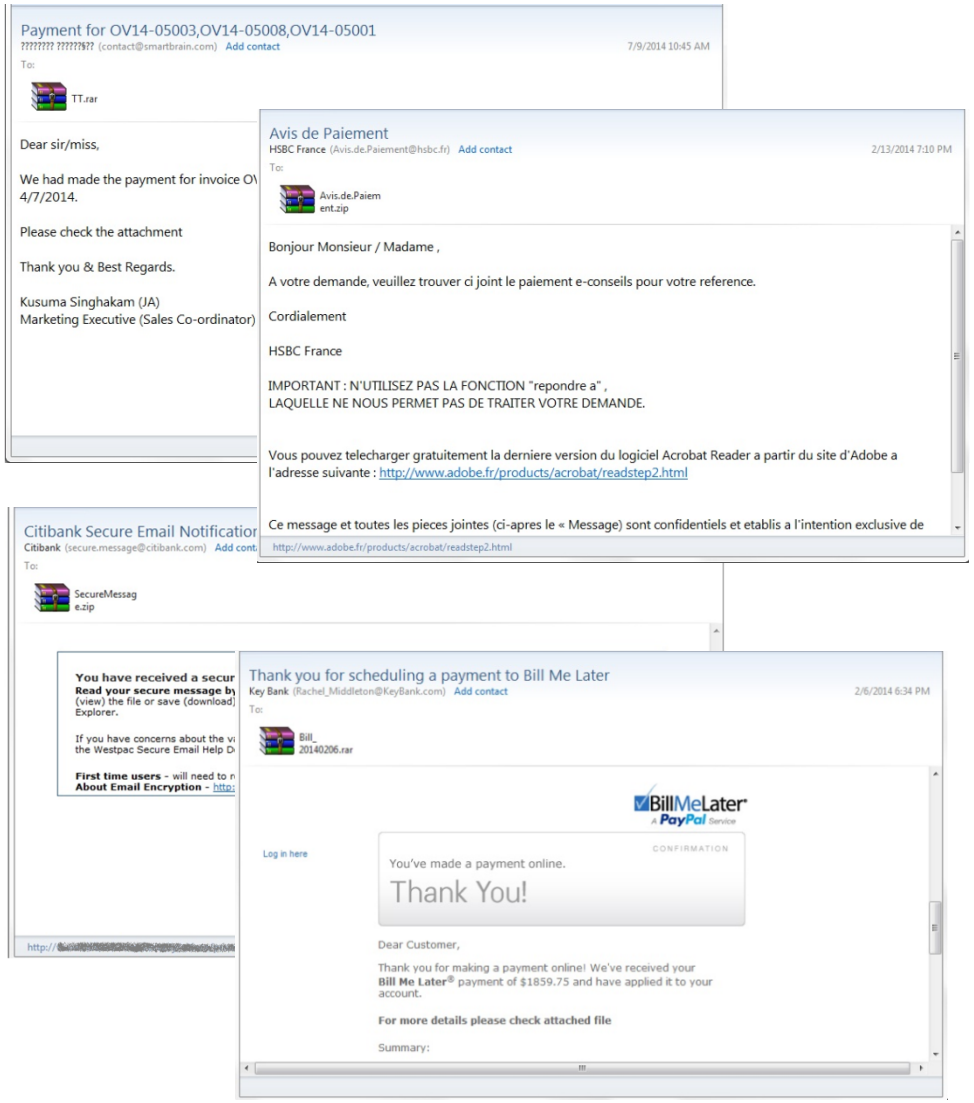
To download and install the newest Updates, follow the instructions on the attached document.
As soon as it is set up, your transaction abilities will be fully restored.

The password to extract the rar document is: Gx2Y14K#

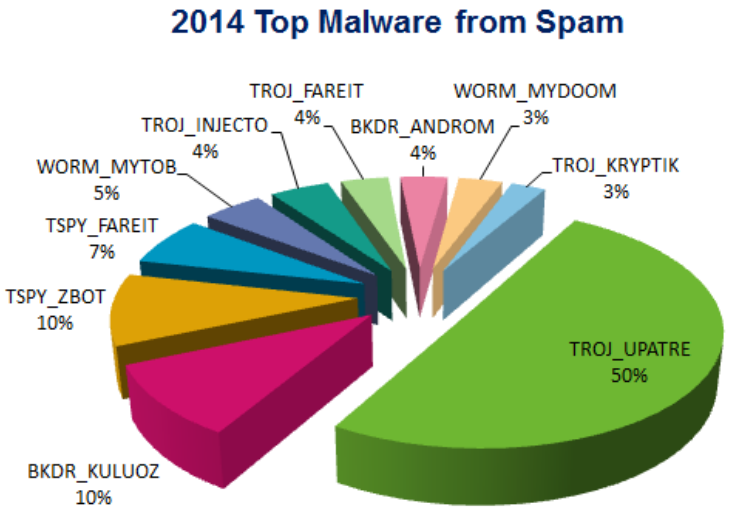
Best regards,
Online security department,
Federal Deposit Insurance Corporation.



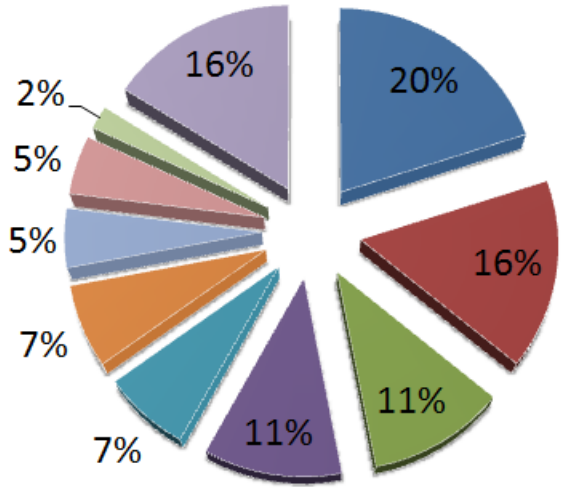
MalSpam With Malicious Attachment



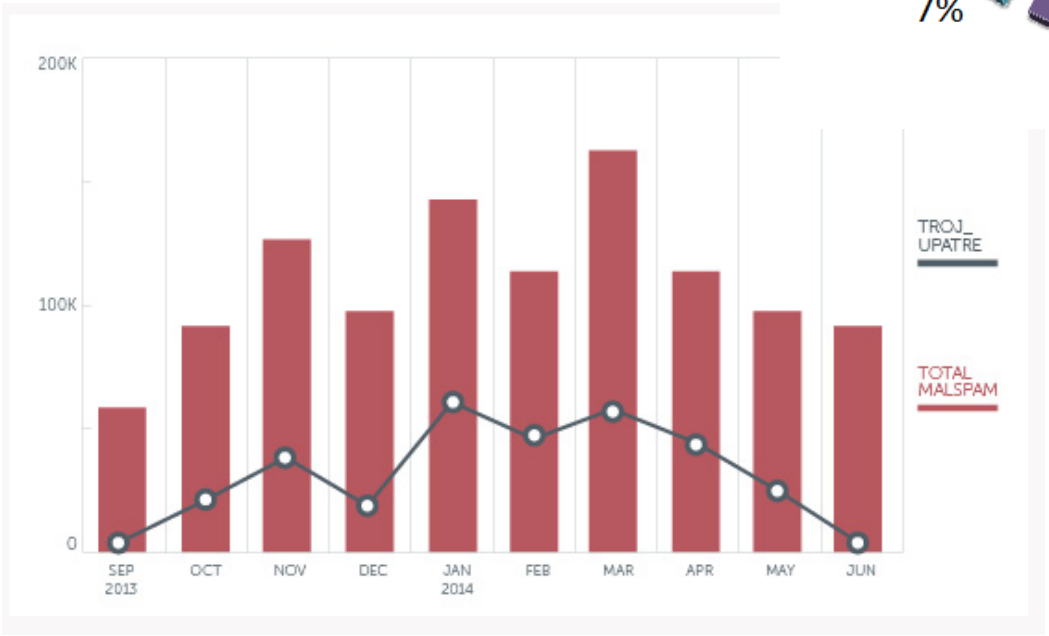
~50% of MalSpam sample carries TROJ_UPATRE variant



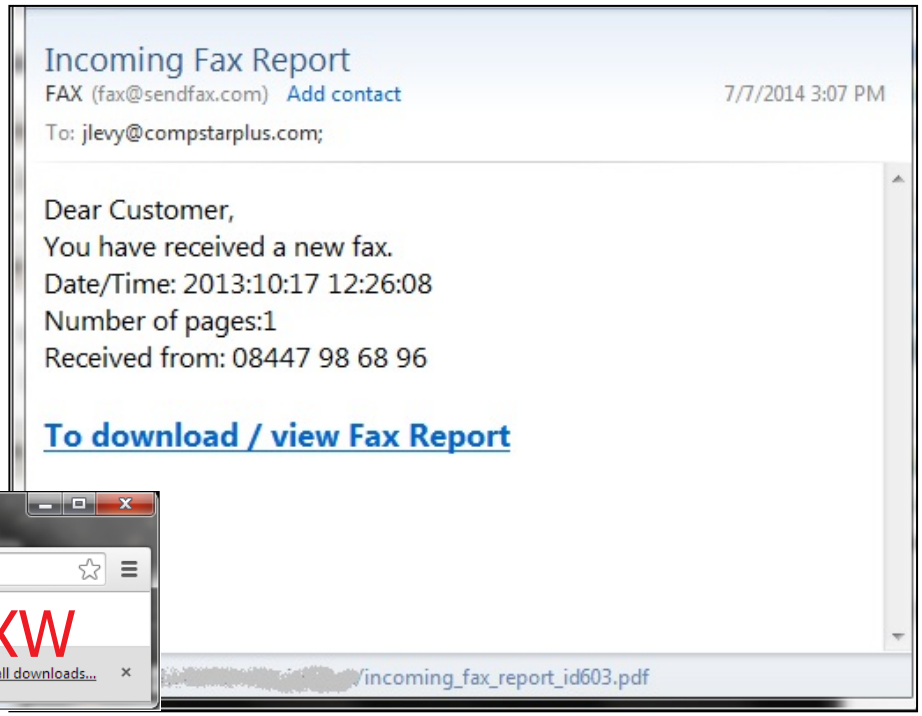
1H – 2014 Top Spam Categories

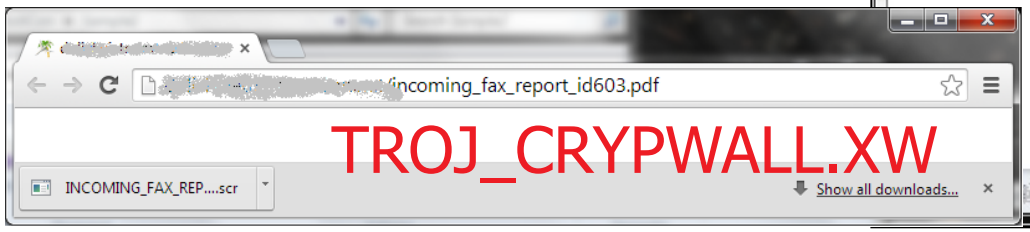


- Malware-related
- Health
- Commercial
- Stocks
- Job
- Adult
- Scams
- Financial
- Education

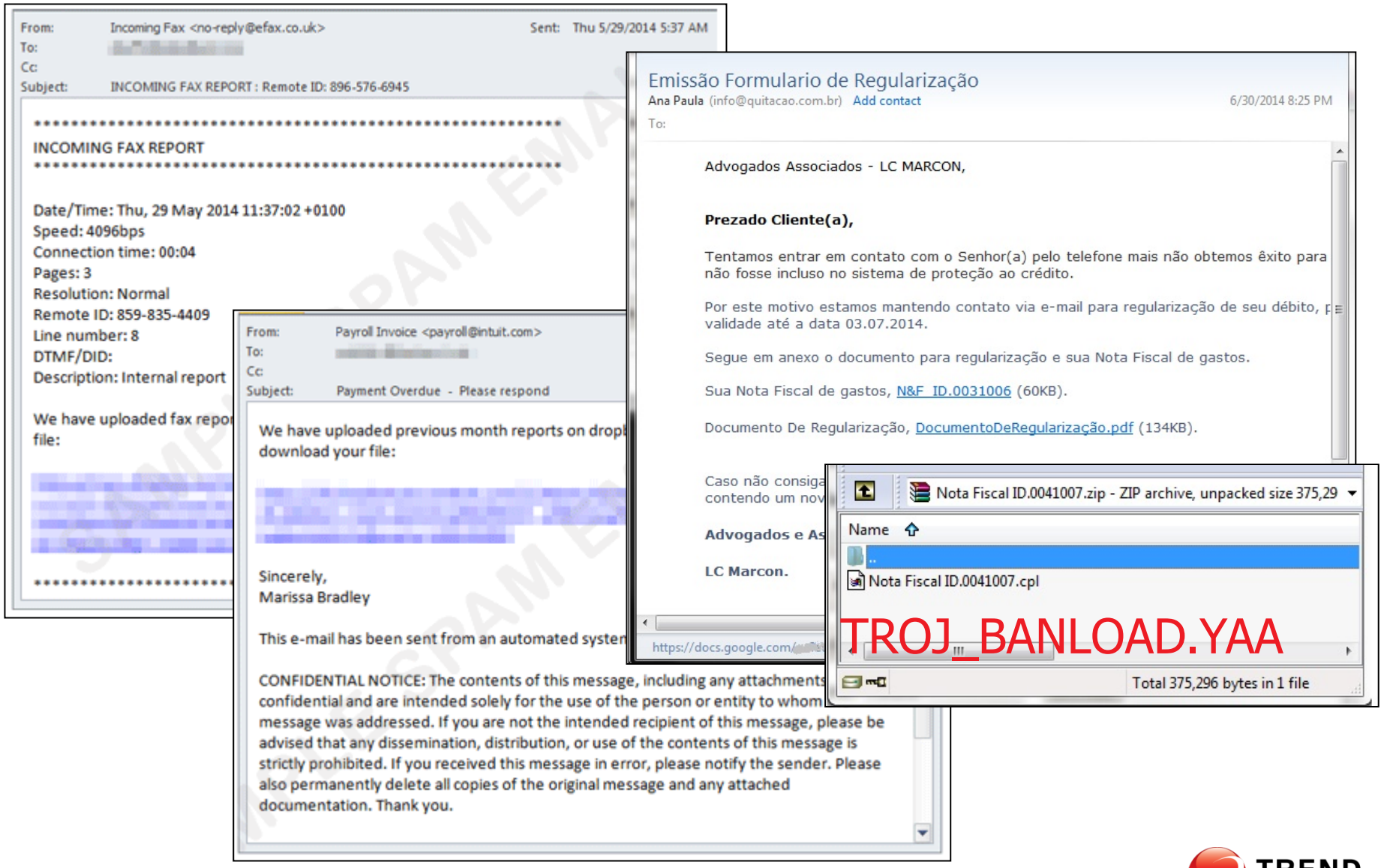


MalSpam with Malicious URL

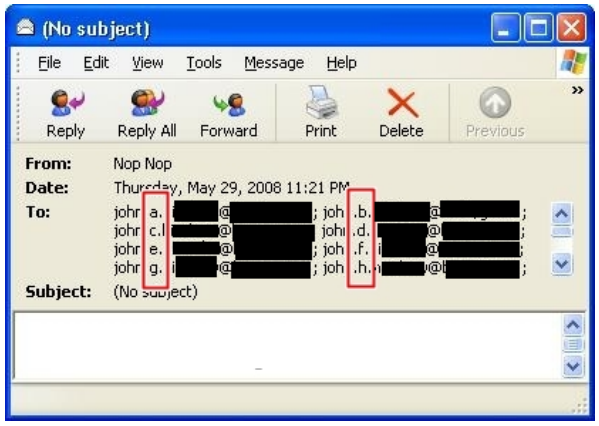


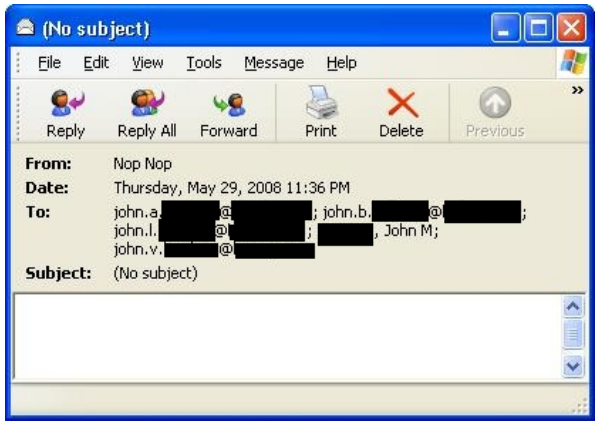


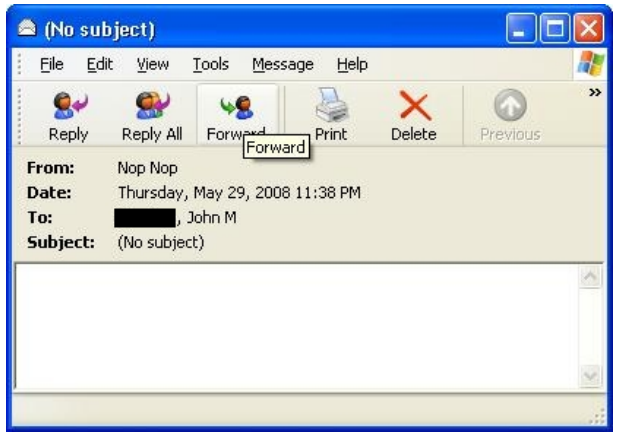
Popular Cloud Services used in MalSpam Campaign



Directory Harvest Attack

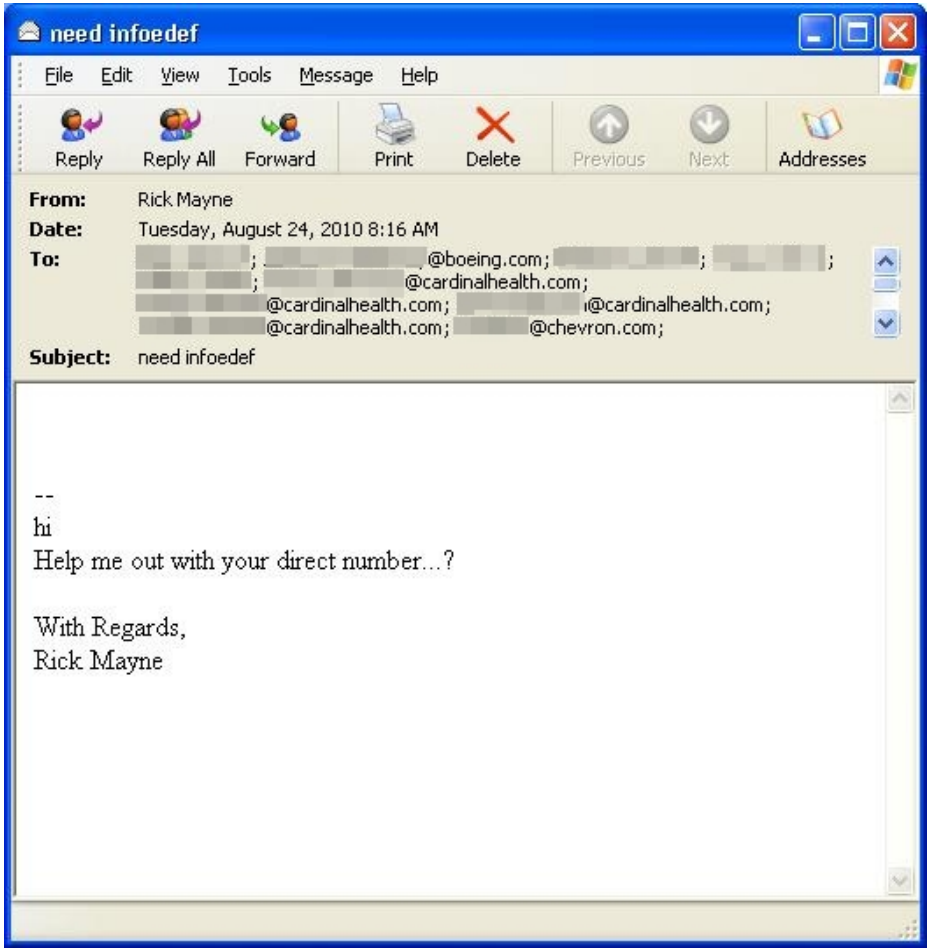


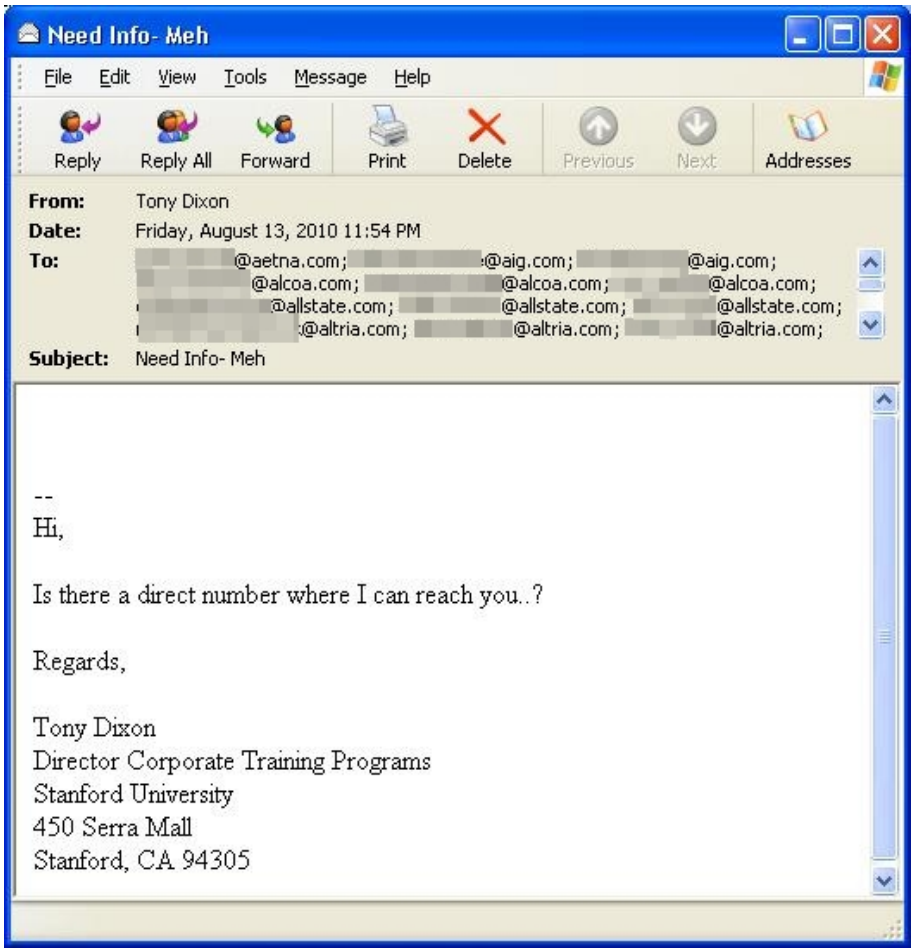




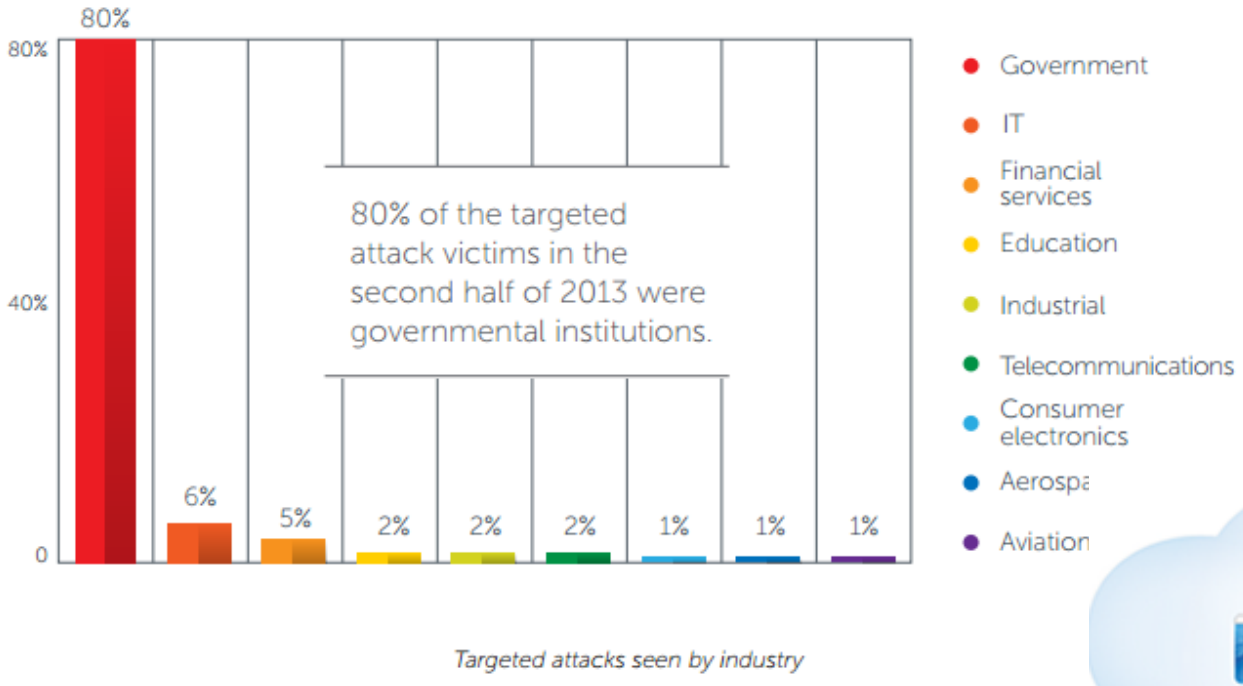
Spam	Timestamp	From	To	Recipients
#1	5/29/08 8:21:04	nopnop32@yahoo.com	john.a.<removed>@<removed>.com - john.z.<removed>@<removed>.com	26
#2	5/29/08 8:36:36	nopnop32@yahoo.com	john.a.<removed>@<removed>.com john.b.<removed>@<removed>.com john.l.<removed>@<removed>.com john.m.<removed>@<removed>.com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





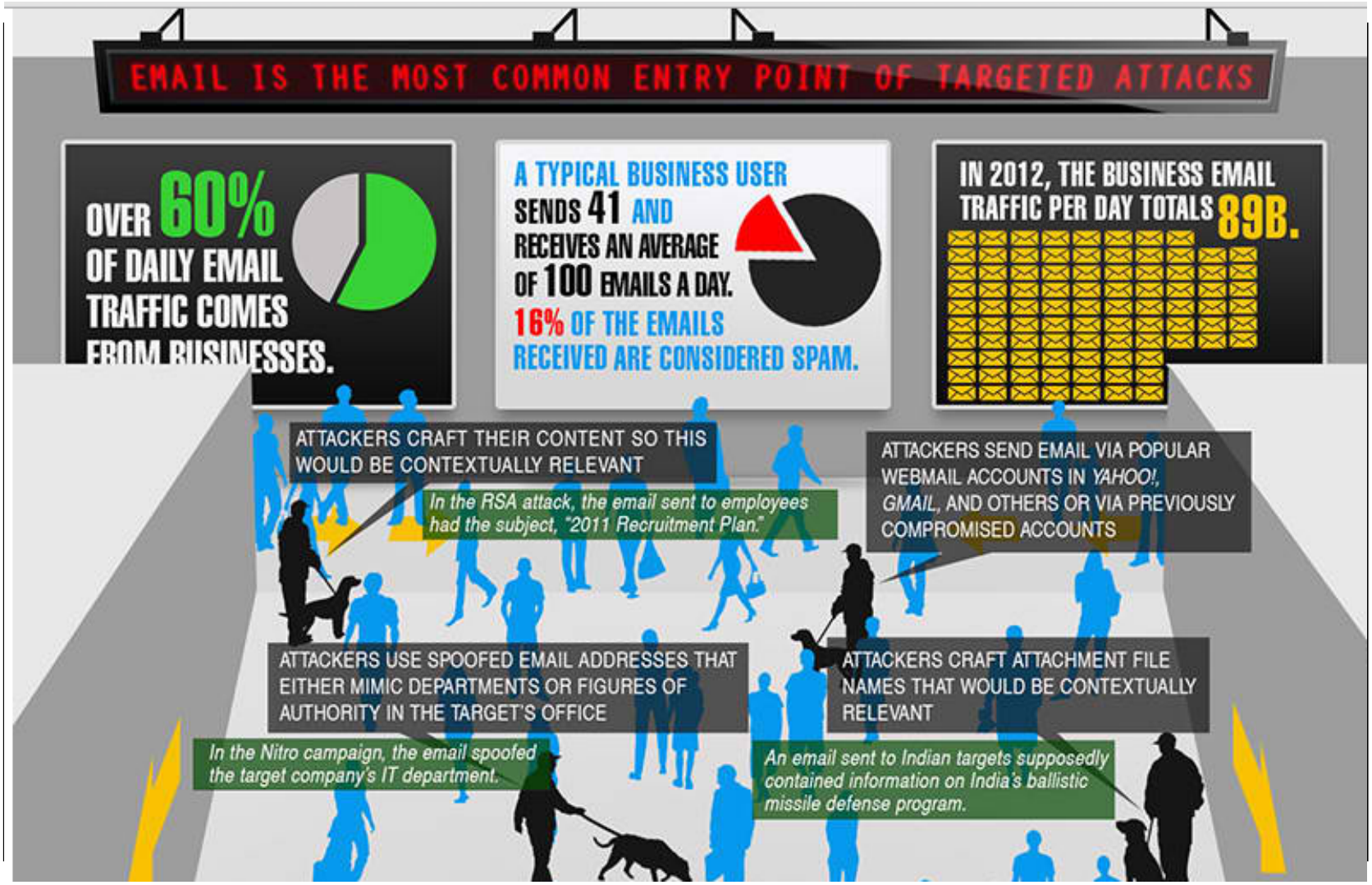
Targeted Attack



Targeted attacks seen by industry

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!