SMS Spam: A Holistic View

“this is the thing we were talking you about *http://bit.ly/1lFFIt3*”

An extended presentation of a paper by

Lamine Aouad, Alejandro Mosquera,
Slawomir Grzonkowski and Dylan Morss from
SECRYPT 2014

@Mobile Messaging Abuse Team

Outline

1. Introduction
2. What SMS spammers do?
3. How to deal with it?
    1. Looking for relevant features
    2. Predicting content variation
    3. Modeling messaging & targeting strategies
4. Use cases
    1. Adult/dating scam
    2. Bank scam
    3. Scams via youtube
    4. Exploiting security features for phishing
5. Conclusions
6. More information about Symantec

1. Introduction

- Disclaimer: financial and legal consequences
- Why does it matter?
- The spam chain
- What do we do/use?
  - Reputation DBs; URL/domains, phone numbers, CTAs
  - Network-based signatures
  - Malware analysis tools
  - Predictive modeling

2. What SMS spammer do?

1. Act/react quickly:
   - Maximize the lifespan of a campaign and react to filtering
     - Blasters can send thousands of messages per second
       - Filtering solutions have a small decision time
     - If a campaign/CTA is blocked: a new message variant, a new CTA, a new target network, reuse it somewhere else,…
2. Stay under-the-radar:
   - Low volume, targeted attacks, and generate user-agent, device- and location-aware responses…
   - Slow-sender vs. fast-sender dilemma:
     - Low-volume campaigns might reach more subscribers in the long term!

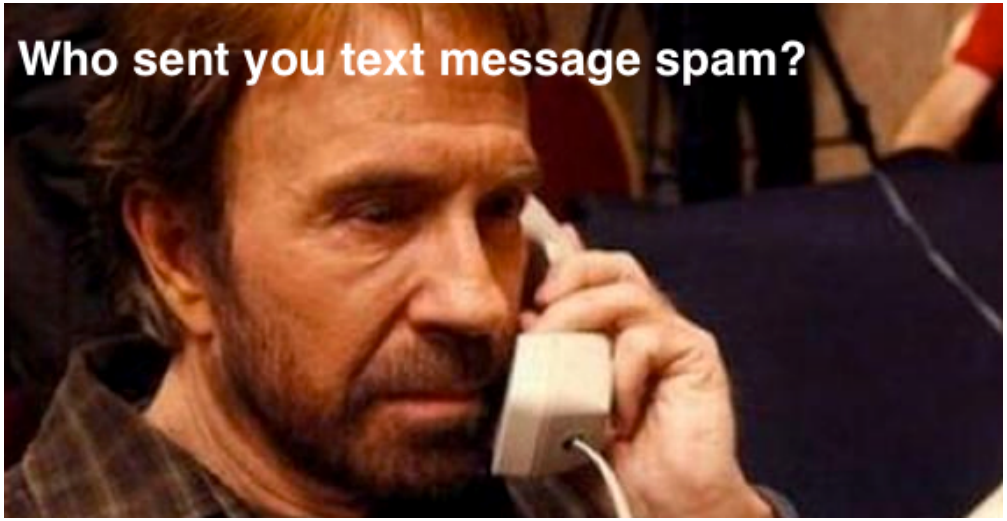
2. What SMS spammers do?

3. Remain cheap:
   - Free hosting, SMS gateways, low cost/free domains…
4. Switch between different products/markets:
   - Choice of campaigns: dating, pharmacy, financial scams, phishing, malware, premium SMS, affiliate or combination of those
5. Don’t repeat content
   - Be creative: polymorphic links, paraphrasing, obfuscation, typo-squatting, newly-registered domains
6. Protect your call-to-action:
   - Use URL shortening services, dynamic-redirection chains…

2. What SMS spammers do?

7. Blame others:
   - Use hacked/compromised websites, fast-flux hosting, dynamic DNS, outsourcing…
8. Pick message recipients in a smart way:
   - Assume neither consecutive or random selection will work
9. If the above doesn't work, pick another target:
   - Traditional email, Craigslist, Twitter, Facebook…

3. How to deal with it?



- Looking for relevant features
- Predicting content
- Modeling targeting strategies

3.1. Looking for relevant features

- If defenses are based only on the final content,

  they will break quickly

- Variation is everywhere! Although more characteristic of the final text content

you can contact us through our website: www.spamdomain1.tk to fill out the Claim
you can contact us through our www.spamdomain2.tk to fill out the Claim
go our website for your claim(www.spamdomain3.tk)or email us your name and address at xx@xx
go to www.spamdomain1.tk, click on claim prize fill the claim form and submit it

- Whether it is the exact same target content or recycled ‘bits and pieces’, it should be used in the filtering
  - Link following and feature extraction are key points here.

3.2. Predicting content variation

- Features extraction in targets using full/partia
  - JavaScript/HTML fingerprints
  - HTTP metadata/headers
  - Redirection flow, cookies
  - Heuristics, and hashing for near-duplicate detection
- Registered new domains/short URLs
  - 70% of the spam uses a URL-based CTA
  - Pre-emptive discovery of URLs/domains
  - Short URL analysis

3.2. Predicting content variation

- In addition of new CTAs, spammers spend a lot generating variants:
  - Paraphrasing, misspelling, contractions, lexical variations, bad grammar, obfuscation and all type of substitutions…
    - Normalization and NLP are key
  - For some recurrent campaigns, regex-fitting has shown to be very effective
- There is no universal classifier and no single most effective method:
  - Generate models for similar campaigns, which will carry the 'right' amount of prediction of new variants

3.3. Modeling targeting strategies

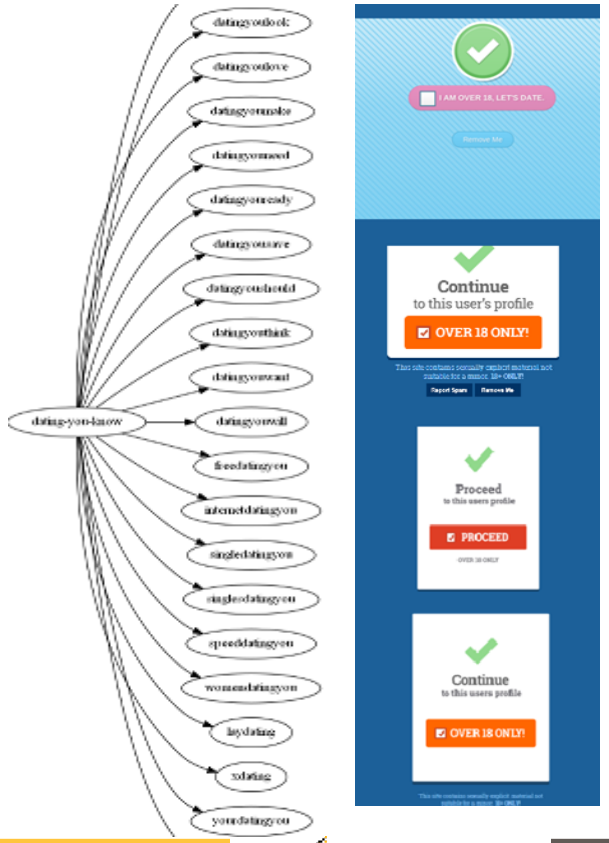
- Fitting uniformly-generated recipients
  - Goodness-of-fit tests
- Mined off the Internet, classified Ads site…
- Sender's reputation:
  - What do we know about senders?
  - Thresholds can be tricky:
    - 5, 10, 30, 50, 100, 500+ messages? Which timeframe?
  - Apps, services, gateways?
- Sending patterns
  - Modeling targeting strategies also takes into account linguistic patterns, call-to-actions, in addition to timestamps

4. Defence use case(s)

- Adult/dating scam
- Bank scam
- Craigslist scams
- Exploiting security features for phishing

4. Defense use case(s)

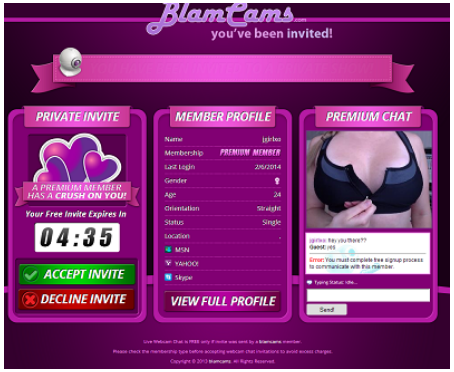
- Adult/dating scam
  - Eroticlove, Xpress, Justhookup, Fuckbook….
  - More than 1300 newly-registered domains redirecting to adult affiliate websites
  - Recurrent domain naming patterns
  - Random generation of recipients
  - Most of these domains are still active and are serving similar content!
  - Reporting to affiliate networks or registrars was not effective: spammers using the same affiliate ID for years!
  - Fast senders, preemptive domain blocking helped to defeat these in SMS, they moved to other targets.



4. Defense use case(s)

- Adult/dating scam
  - Webcammatches.com affiliates: started with newly-registered domains but moved to social media (tumblr)
  - Still active using bots!

so i don't have xrated pics online but i have a couple on my phone... purplegigglefffus.tumblr.com/aaj5byy.jpg ... now send me urs bby
my turn.. purplegigglefffus.tumblr.com/abpyuty.jpg .. u like :-)
last 1 baby purplegigglefffus.tumblr.com/acqtazl.jpg , you know you want this
or just join through my page so u dont pay purplegigglefffus.tumblr.com/invite/yh78 thats my page



  - There is not always a call to action in the message, sending patterns help to detect these:

its supposed to be the best App for this kind of thing, hurry up and accept!!!
yea i'm a member so you dont pay, wait until u see what we can do when you are in ;)
its free to join but it will ask for a card i think.. im gonna get naughty and i cant have kids watching..
ok babe.. talk to you in there.. gonna put my phone to charge.. mwa! xoxo

4. Defense use case(s)

- Bank scam
  - One of the longest running campaigns that changes every week:
    - Different CTAs: phone numbers
    - Different messages: template-based variation

BANK UPDATE: YOUR CARD #435547XXXXXX HAS BEEN TEMPORARILY DEACTIVATED.TO REACTIVATE, Please call: 205-xxx-xxx.
BANK UPDATE: YOUR CARD #435547XXXXXX HAS BEEN TEMPORARILY DEACTIVATED.TO REACTIVATE, Please call: 423-xxx-xxx.
CREDIT UNION BANK ALERT: YOUR CARD #435547 HAS BEEN TEMPORARILY DEACTIVATED.TO REACTIVATE, Please call: 423-xxx-xxx.
JEFFERSON FEDERAL BANK ALERT: YOUR CARD #486168 HAS BEEN TEMPORARILY DEACTIVATED.TO REACTIVATE, Please call: 423-xxx-xxx.
REGIONS BANK ALERT: YOUR CARD #435XXXXXX HAS BEEN TEMPORARILY DEACTIVATED.TO REACTIVATE, Please call: 615-xxx-xxx
REGIONS BANK ALERT: Your VISA #435547 has been temporarily DEACTIVATED. Please call Regions Bank 24hrs line (205) xxx-xxx
"South Side Bank ALERT: Your VISA #433152 has been temporarily DEACTIVATED. Please call our 24hrs line (309) xxx-xxx"
(CREDIT UNION) Your Visa Card has been temporary BLOCK. Do to Our Security Updates. Please Call our 24hr Service line at 440-xxx-xxx
(FIRST NATIONAL BANK ALERT) Your VISA CARD 460717 has been temporarily Block. Please contact Us at (931)210-8021 to reactivate
(FIRST TENNESSEE BANK ALERT) Your CARD has been temporarily DEACTIVATED. Please call FIRST TENNESSEE Bank Card Services at (901) xxx-xxxto reactivate
(FW: REGIONS BANK ALERT) Your VISA CARD has been temporarily DEACTIVATED. Please call Regions Bank Card Services at 205-xxx-xxx to reactivate
(JEFFERSON FEDERAL BANK ALERT) Your CARD #486168 has been temporarily DEACTIVATED. Please call Jefferson Bank at 423-xxx-xxxto reactivate
(LANSING AUTOMAKER ALERT) Your Master Card 551053 has been temporary BLOCK. Do to Our Security Updates. Please contact us at 517-xxx-xxx
(LANSING AUTOMAKER ALERT) Your Master Card 551053 has been temporary BLOCKED. Do to Our Security Updates. Please contact us at 517-xxx-xxx
(MECU ALERT) Your Card Visa has been temporary BLOCK. Do to Our Security Updates. Please Call MUNICIPAL EMPLOYEES at 410-xxx-xxx

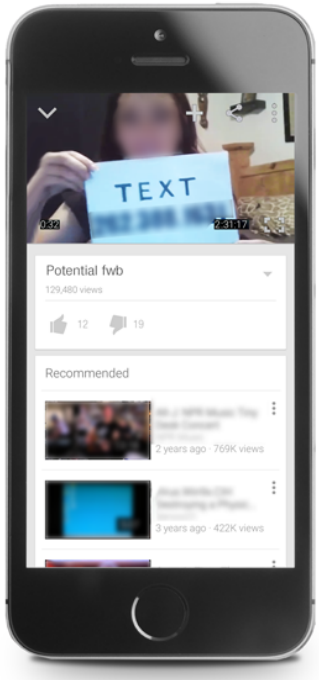
  - NLP models and regexes are quite effective against this one

4. Defense use case(s)

- Craigslist scams
  - There are numerous scams targeting legitimate websites such as craigslist
  - Scam and phishing campaigns containing URL,

  Phone numbers or some other characteristics are quite well detected
  - Occasionally we observe new evasion techniques
  - One of the recent ones included distributing a link to

  a youtube video that was directing to the phone number of the



4. Defense use case(s)

- Exploiting security features for phishing
  - Why to ask for password if an account can be hijacked with just one evil SMS?
  - We observe more and more attacks where the attacker knows the username and phone number of the victim
  - Then the attacker initiate the password recovery process and after a while send one message, e.g.,

    "Please reply with the new code we have sent to verify your identity. Failure will put a permanent lock on your account."

  - In most cases if the victim responds with this code, the account is lost.

5. Conclusions

- An increasing level of sophistication
- Smaller and more targeted campaigns
  - Keeping under-the-radar!
- They are multi-channels but not abandoning the SMS channel yet despite the lower volume overall

- In terms of filtering; link following at different levels of granularity is key!
- Targeted and constantly tuned predictive models

5. References

- SMS Spam: A Holistic View. L Aouad, A Mosquera, S Grzonkowski, D Morss. In Proceedings of SECRYPT 2014 - The International Conference on Security and Cryptography.
- SMS spammers hide adult site URLs in YouTube videos
  - http://www.symantec.com/connect/blogs/sms-spammers-hide-adult-site-urls-youtube-videos
- Password recovery scam tricks users into handing over email account access
  - http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access
- On Detecting Messaging Abuse in Short Text Messages using Linguistic and Behavioral patterns. A Mosquera, L Aouad, S Grzonkowski, D Morss. arXiv preprint arXiv:1408.3934
- Smartphone Security: An overview of emerging threats. S Grzonkowski, A Mosquera, L Aouad, D Morss. Consumer Electronics Magazine, IEEE 3 (4), 40-44

Symantec

- It was founded in 1982 and since then it has acquired a number of companies, e.g., PGP or Verisign
- Mostly recognized through its Norton Antivirus product
- As announced in October 2014, the company would split into two independent publicly traded companies by the end of 2015
  - One company would focus on security
  - The other on information management
  - The information-management business will use the name Veritas

Annual summary of relevant threats: Internet Security Threat Report

Relevant areas of interests for the last year include:

- Mobile devices and Internet of Things
  - Mobile apps
  - SMS threats
- Web Threats
  - Heartbleed
  - Shellshock
  - Poodle
  - Malvertising
- Social Media & Scams
  - Targeting popular social websites
  - affiliate programs
  - Dating scams

Annual summary of relevant threats: Internet Security Threat Report

Relevant areas of interests:

- Targeted Attacks
  - Zero-day vulnerabilities
  - Cyber espionage
  - Watering hole
  - Threat intelligence
- Data Breaches and Privacy
  - Data security
  - Data breaches
- E-crime and Malware
  - Ransomware and cryptolockers
  - Underground economy

Opportunities at Symantec

- Good background in computer science
- Creative thinking
- Security oriented mind
- Experience with security tools and frameworks

Thank you