网络测量研究的案例分析

刘保君

2020年11月10日

1. Common Sense

2. Case Studies

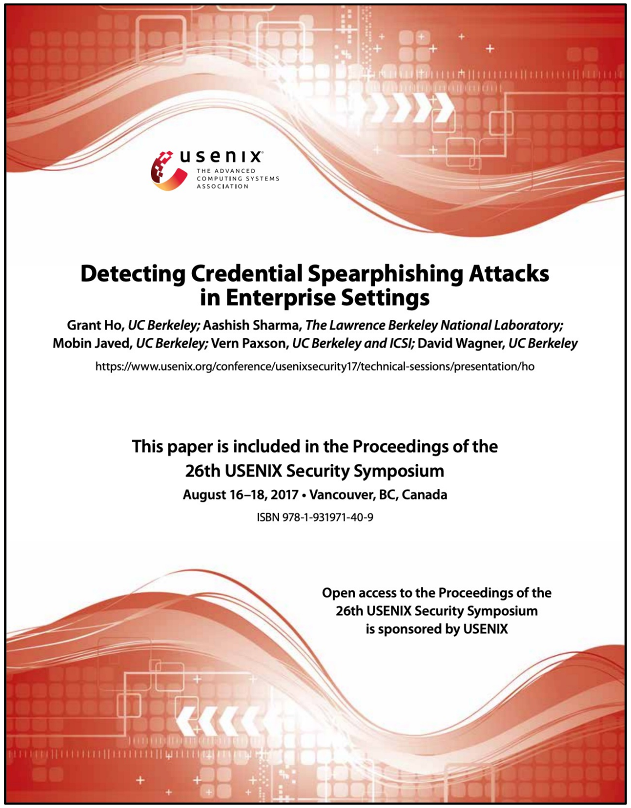
3. Some Tips

1. **Common Sense**

2. Case Studies

3. Some Tips

Common Sense



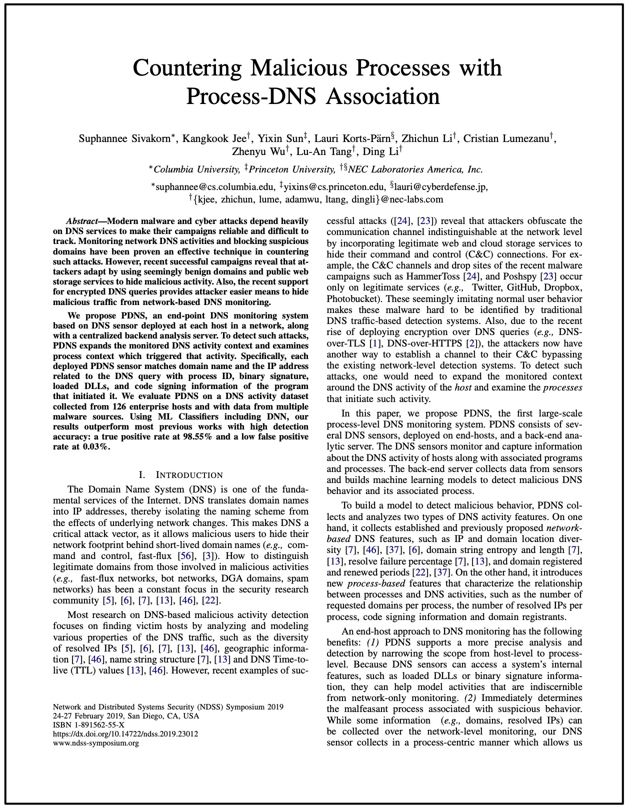
Detecting Credential Spearphishing Attacks in Enterprise Settings

Grant Ho, *UC Berkeley;* Aashish Sharma, *The Lawrence Berkeley National Laboratory;* Mobin Javed, *UC Berkeley;* Vern Paxson, *UC Berkeley and ICSI;* David Wagner, *UC Berkeley*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ho

This paper is included in the Proceedings of the
26th USENIX Security Symposium
August 16–18, 2017 • Vancouver, BC, Canada
ISBN 978-1-931971-40-9

Open access to the Proceedings of the
26th USENIX Security Symposium
is sponsored by USENIX



Countering Malicious Processes with Process-DNS Association

Suphannee Sivakorn*, Kangkook Jee†, Yixin Sun‡, Lauri Korts-Pärn§, Zhichun Li†, Cristian Lumezanu†,
Zhenyu Wu†, Lu-An Tang†, Ding Li†

**Columbia University,* ‡*Princeton University,* †§*NEC Laboratories America, Inc.*

*suphannee@cs.columbia.edu, ‡yixins@cs.princeton.edu, §lauri@cyberdefense.jp,
†{kjee, zhichun, lume, adamwu, ltang, dingli}@nec-labs.com

***Abstract*—Modern malware and cyber attacks depend heavily on DNS services to make their campaigns reliable and difficult to track. Monitoring network DNS activities and blocking suspicious domains have been proven an effective technique in countering such attacks. However, recent successful campaigns reveal that attackers adapt by using seemingly benign domains and public web storage services to hide malicious activity. Also, the recent support for encrypted DNS queries provides attacker easier means to hide malicious traffic from network-based DNS monitoring.**

We propose PDNS, an end-point DNS monitoring system based on DNS sensor deployed at each host in a network, along with a centralized backend analysis server. To detect such attacks, PDNS expands the monitored DNS activity context and examines process context which triggered that activity. Specifically, each deployed PDNS sensor matches domain name and the IP address related to the DNS query with process ID, binary signature, loaded DLLs, and code signing information of the program that initiated it. We evaluate PDNS on a DNS activity dataset collected from 126 enterprise hosts and with data from multiple malware sources. Using ML Classifiers including DNN, our results outperform most previous works with high detection accuracy: a true positive rate at 98.55% and a low false positive rate at 0.03%.

I. Introduction

The Domain Name System (DNS) is one of the fundamental services of the Internet. DNS translates domain names into IP addresses, thereby isolating the naming scheme from the effects of underlying network changes. This makes DNS a critical attack vector, as it allows malicious users to hide their network footprint behind short-lived domain names (*e.g.,* command and control, fast-flux [56], [3]). How to distinguish legitimate domains from those involved in malicious activities (*e.g.,* fast-flux networks, bot networks, DGA domains, spam networks) has been a constant focus in the security research community [5], [6], [7], [13], [46], [22].

Most research on DNS-based malicious activity detection focuses on finding victim hosts by analyzing and modeling various properties of the DNS traffic, such as the diversity of resolved IPs [5], [6], [7], [13], [46], geographic information [7], [46], name string structure [7], [13] and DNS Time-to-live (TTL) values [13], [46]. However, recent examples of successful attacks ([24], [23]) reveal that attackers obfuscate the communication channel indistinguishable at the network level by incorporating legitimate web and cloud storage services to hide their command and control (C&C) connections. For example, the C&C channels and drop sites of the recent malware campaigns such as HammerToss [24], and Poshspy [23] occur only on legitimate services (*e.g.,* Twitter, GitHub, Dropbox, Photobucket). These seemingly imitating normal user behavior makes these malware hard to be identified by traditional DNS traffic-based detection systems. Also, due to the recent rise of deploying encryption over DNS queries (*e.g.,* DNS-over-TLS [1], DNS-over-HTTPS [2]), the attackers now have another way to establish a channel to their C&C bypassing the existing network-level detection systems. To detect such attacks, one would need to expand the monitored context around the DNS activity of the *host* and examine the *processes* that initiate such activity.

In this paper, we propose PDNS, the first large-scale process-level DNS monitoring system. PDNS consists of several DNS sensors, deployed on end-hosts, and a back-end analytic server. The DNS sensors monitor and capture information about the DNS activity of hosts along with associated programs and processes. The back-end server collects data from sensors and builds machine learning models to detect malicious DNS behavior and its associated process.

To build a model to detect malicious behavior, PDNS collects and analyzes two types of DNS activity features. On one hand, it collects established and previously proposed *network-based* DNS features, such as IP and domain location diversity [7], [46], [37], [6], domain string entropy and length [7], [13], resolve failure percentage [7], [13], and domain registered and renewed periods [22], [37]. On the other hand, it introduces new *process-based* features that characterize the relationship between processes and DNS activities, such as the number of requested domains per process, the number of resolved IPs per process, code signing information and domain registrants.

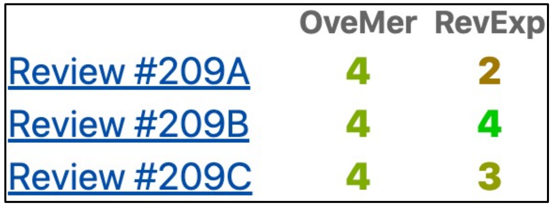
An end-host approach to DNS monitoring has the following benefits: *(1)* PDNS supports a more precise analysis and detection by narrowing the scope from host-level to process-level. Because DNS sensors can access a system's internal features, such as loaded DLLs or binary signature information, they can help model activities that are indiscernible from network-only monitoring. *(2)* Immediately determines the malfeasant process associated with suspicious behavior. While some information (*e.g.,* domains, resolved IPs) can be collected over the network-level monitoring, our DNS sensor collects in a process-centric manner which allows us

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23012
www.ndss-symposium.org

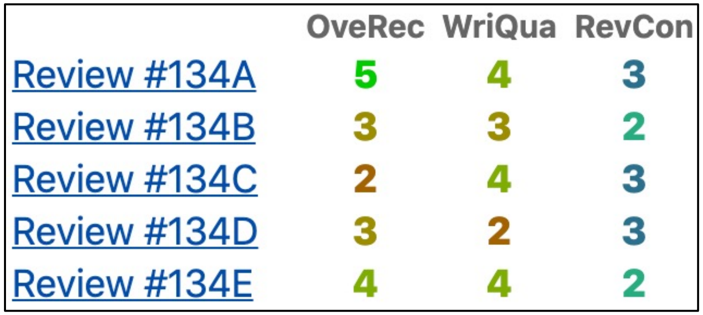
USENIX Security
Best Paper Award

NDSS
Bottom Line Paper

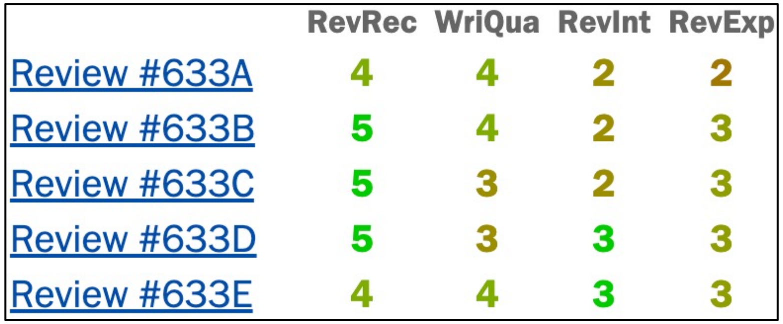
Evaluation Criteria



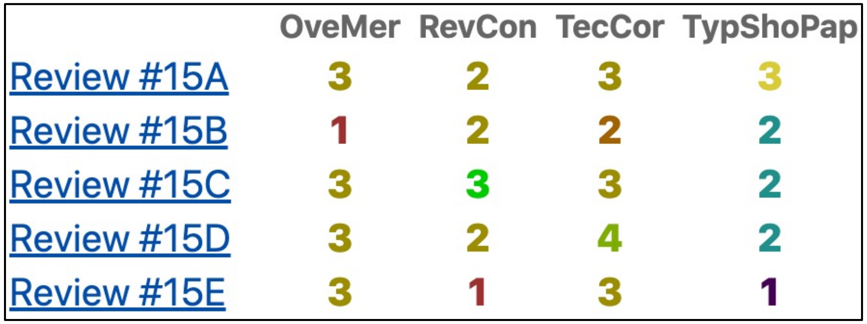
	OveMer	RevExp
Review #209A	4	2
Review #209B	4	4
Review #209C	4	3



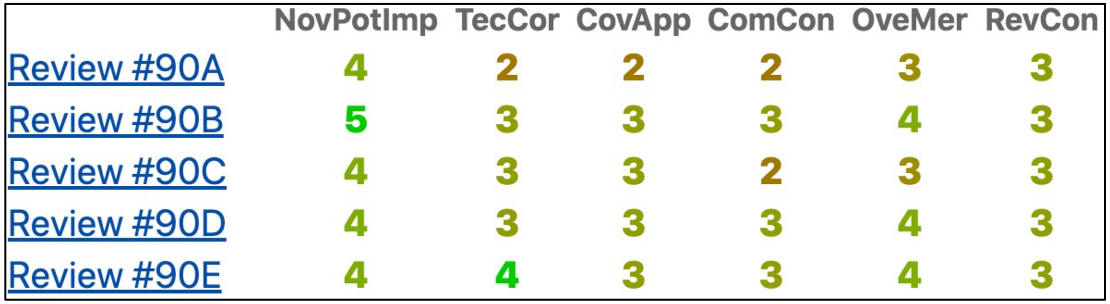
	OveRec	WriQua	RevCon
Review #134A	5	4	3
Review #134B	3	3	2
Review #134C	2	4	3
Review #134D	3	2	3
Review #134E	4	4	2



	RevRec	WriQua	RevInt	RevExp
Review #633A	4	4	2	2
Review #633B	5	4	2	3
Review #633C	5	3	2	3
Review #633D	5	3	3	3
Review #633E	4	4	3	3



	OveMer	RevCon	TecCor	TypShoPap
Review #15A	3	2	3	3
Review #15B	1	2	2	2
Review #15C	3	3	3	2
Review #15D	3	2	4	2
Review #15E	3	1	3	1



	NovPotImp	TecCor	CovApp	ComCon	OveMer	RevCon
Review #90A	4	2	2	2	3	3
Review #90B	5	3	3	3	4	3
Review #90C	4	3	3	2	3	3
Review #90D	4	3	3	3	4	3
Review #90E	4	4	3	3	4	3

Evaluation Criteria

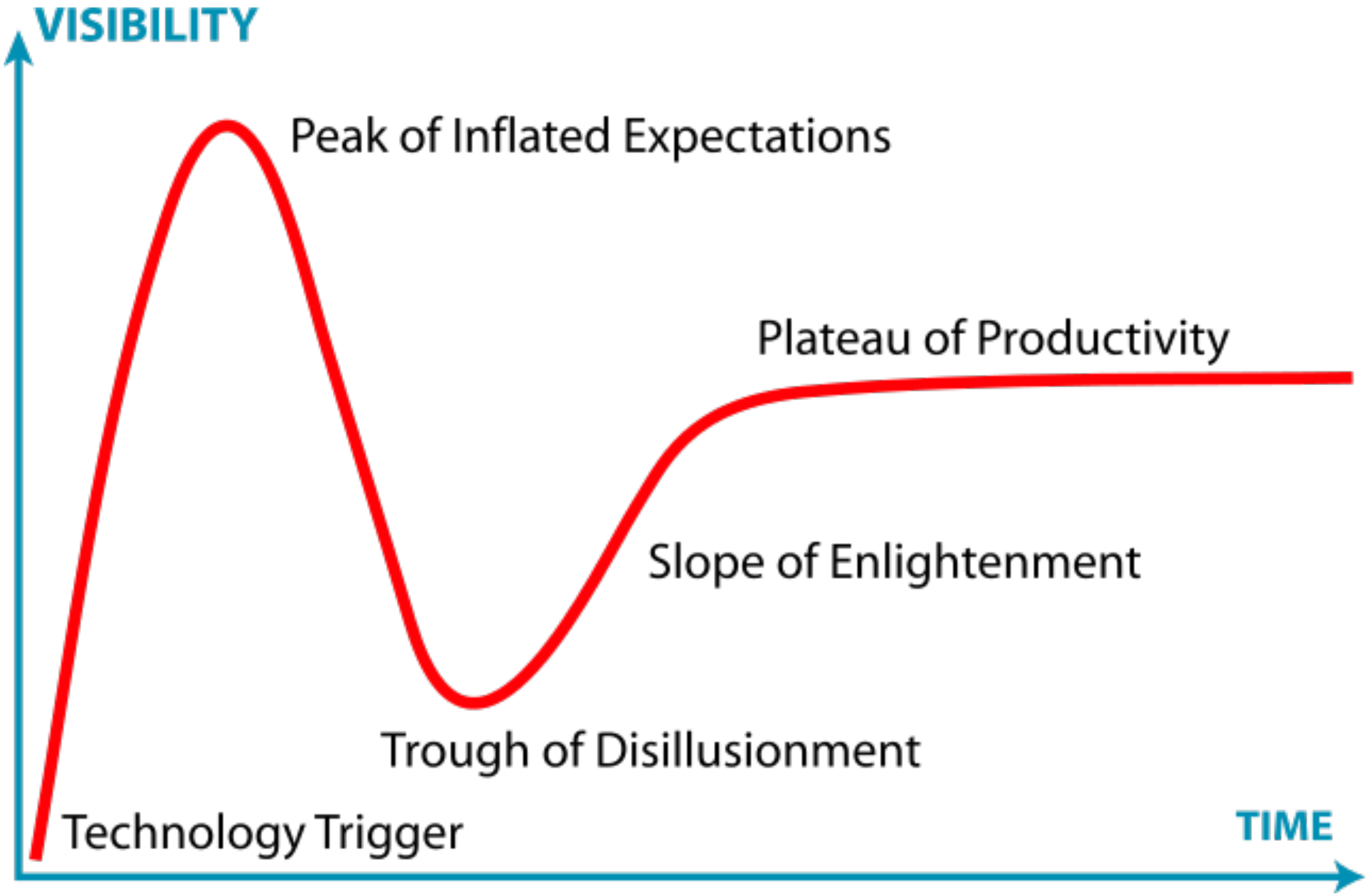
- **Overall merit**
- **Novelty and potential for impact**
- **Technical correctness**
- **Coverage/applicability**
- **Community contribution**
- **Writing quality**
- **Reviewer interest**

Evaluation Criteria

- ❑ Novel Problem
- ❑ Solid Work
- ❑ Well Written

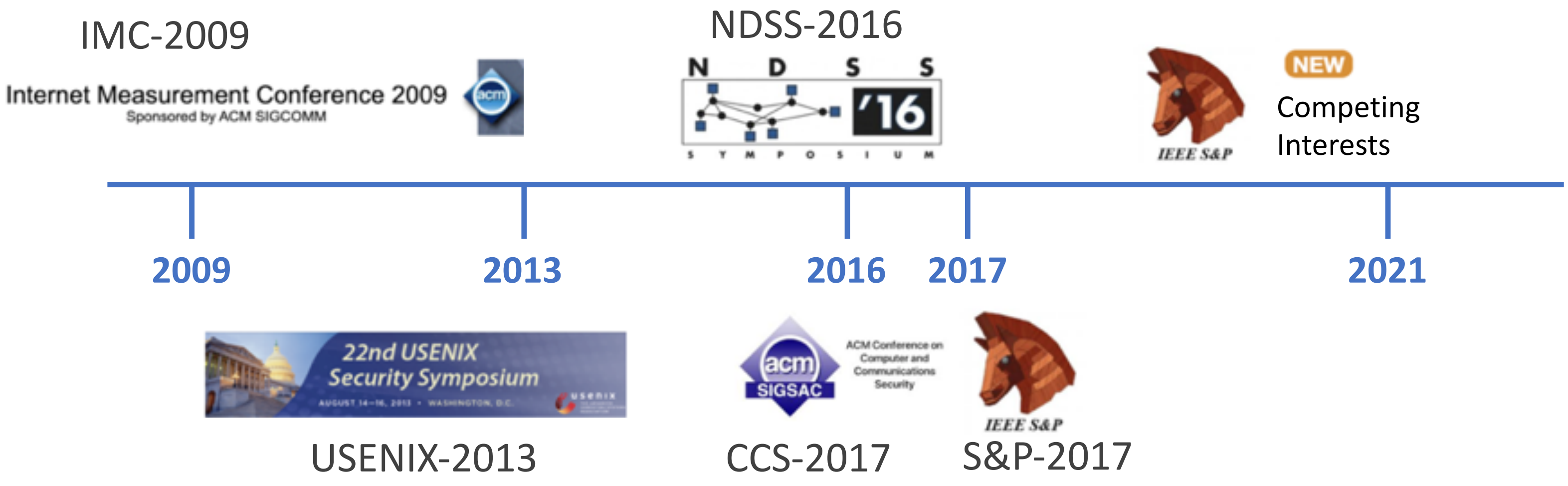
Research Scope

Good Idea


VISIBILITY
Peak of Inflated Expectations
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

Ethical Considerations

- Researches of human subjects: **Must** approved by **IRB**
  - Network Measurement
  - Censorship Measurement
  - Data Sharing



IMC-2009

NDSS-2016

NEW

Competing Interests

2009

2013

2016

2017

2021

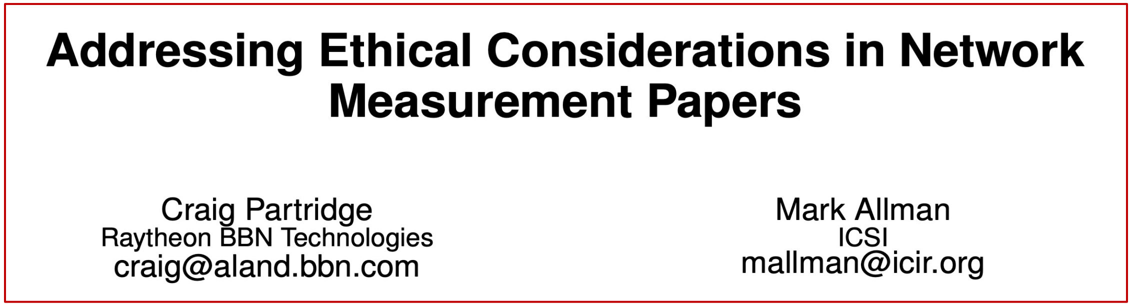
USENIX-2013

CCS-2017

S&P-2017

Internet Measurement Conference 2009
Sponsored by ACM SIGCOMM
acm
N D S S '16
S Y M P O S I U M
IEEE S&P
22nd USENIX Security Symposium
AUGUST 14–16, 2013 • WASHINGTON, D.C.
usenix
acm SIGSAC
ACM Conference on Computer and Communications Security
IEEE S&P

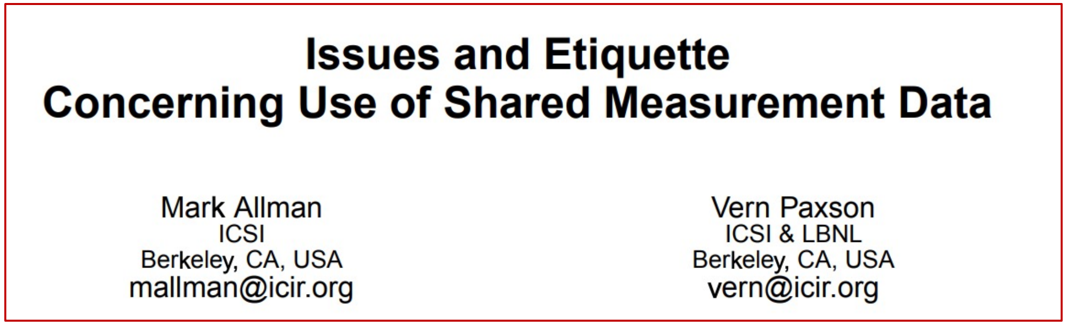
Ethical Considerations



Addressing Ethical Considerations in Network Measurement Papers

Craig Partridge
Raytheon BBN Technologies
craig@aland.bbn.com

Mark Allman
ICSI
mallman@icir.org



Issues and Etiquette Concerning Use of Shared Measurement Data

Mark Allman
ICSI
Berkeley, CA, USA
mallman@icir.org

Vern Paxson
ICSI & LBNL
Berkeley, CA, USA
vern@icir.org

The Menlo Report

Ethical Principles Guiding Information and Communication Technology Research

August 2012

Homeland Security
Science and Technology

Ethical Considerations

Paper Space devoted to discussions related to ethical issues

1. Common Sense

2. **Case Studies**

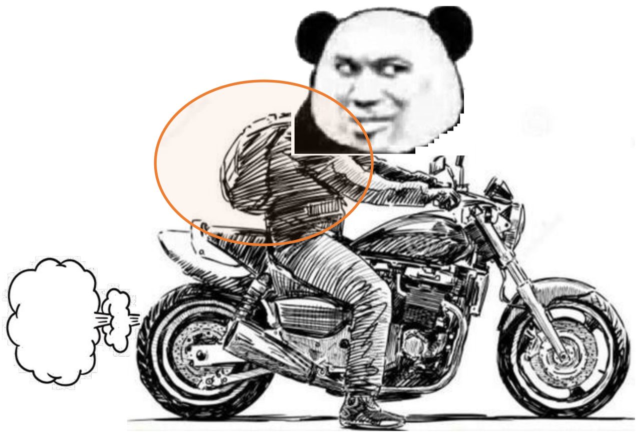
3. Some Tips

Project:

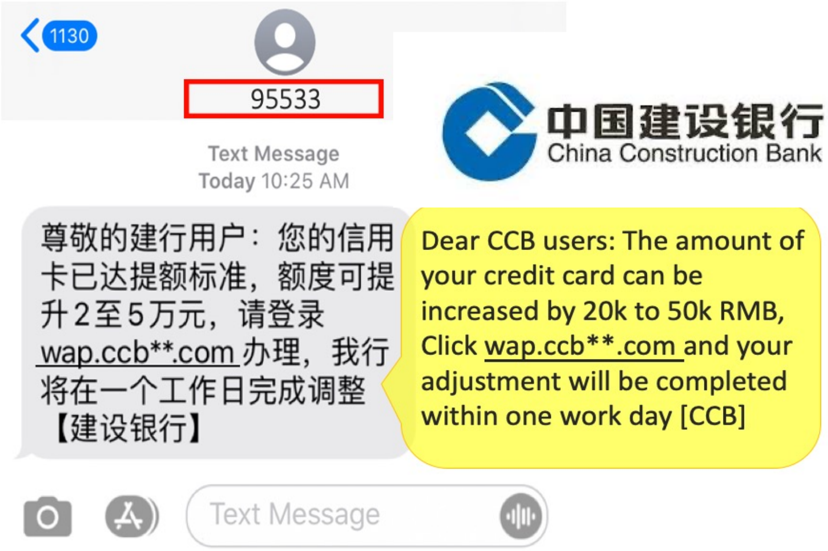
Fake-base-station Spam Ecosystem

Fake-base-station is right by your side

Victim



FBS Operator/Spammer



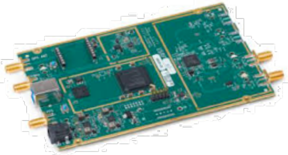
95533

Text Message
Today 10:25 AM

尊敬的建行用户：您的信用卡已达提额标准，额度可提升2至5万元，请登录wap.ccb**.com办理，我行将在一个工作日完成调整【建设银行】

Dear CCB users: The amount of your credit card can be increased by 20k to 50k RMB, Click wap.ccb**.com and your adjustment will be completed within one work day [CCB]

FBS Spam Message

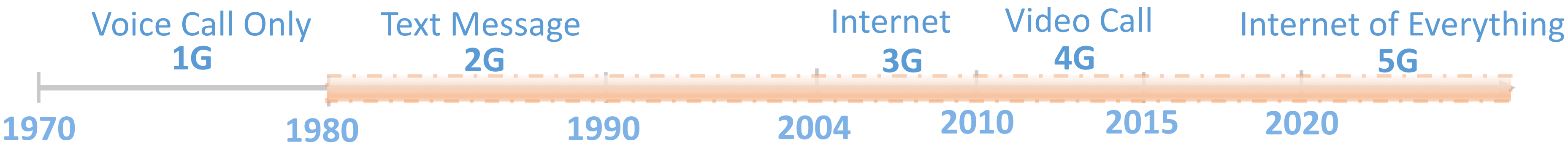


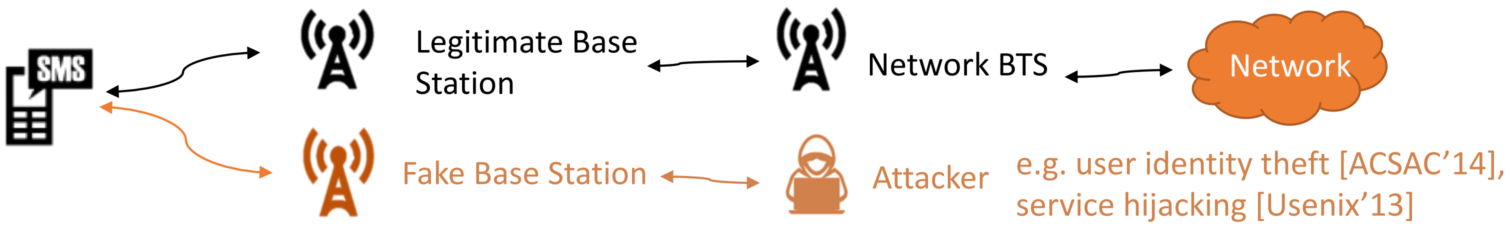
Software-defined radio (SDR)

Laptop

FBS Devices

FBS: A Long-standing Problem





e.g. user identity theft [ACSAC’14], service hijacking [Usenix’13]

Root Cause: **Lack of base station authentication** under GSM(2G) network

An adversary could force the device to **downgrade from 3G/4G(5G) to 2G.**

FBS will be a **long-standing threat** !

FBS as a Spamming Channel

- In this work, we focus on the ability of FBSes to *send spam messages* to end-user devices *from arbitrary phone numbers*.

Previous Work

Focus on detecting FBSes

Strong Signal Strength

Significant Change of BS ID

Similar features were used to collect data in this work*

Motivation

To understand the fraudulent activities and explore strategies in the FBS spam ecosystem through a **data-driven approach**

279K real-world FBS messages in China (largest known dataset)

* The data collection was implemented by our **industrial partner**, and *we don't consider it as our contribution in this work.*

FBS as a Spamming Channel

- In this work, we focus on the ability of FBSes to *send spam messages* to end-user devices *from arbitrary phone numbers*.

Previous Work

Focus on detecting FBSes

Strong Signal Strength

Significant Change of BS ID

Similar features were used to collect data in this work*

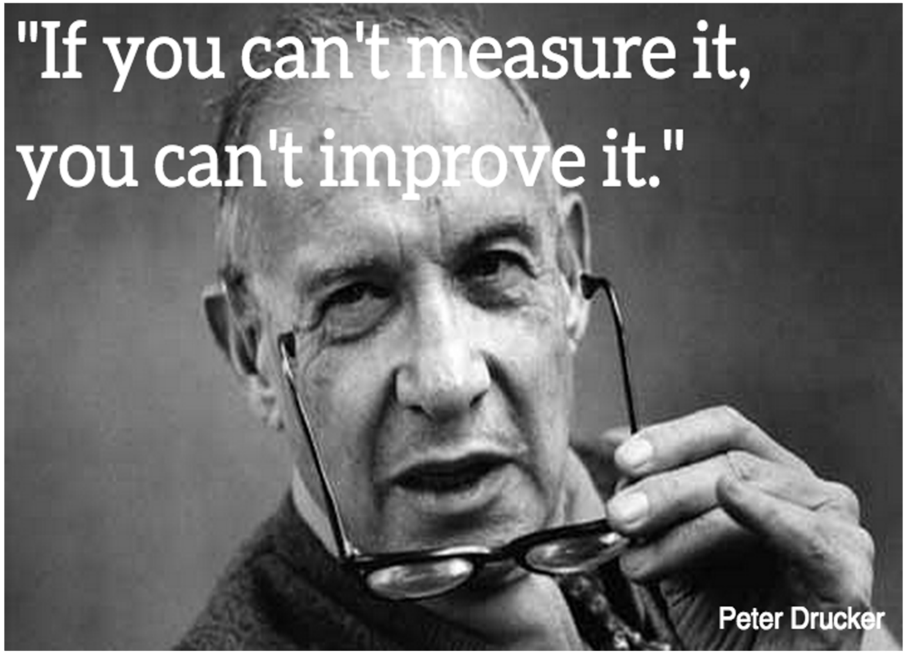
We still lack deep insights into the ecosystem powered by FBSes.

Motivation

279K real-world FBS messages in China (largest known dataset)

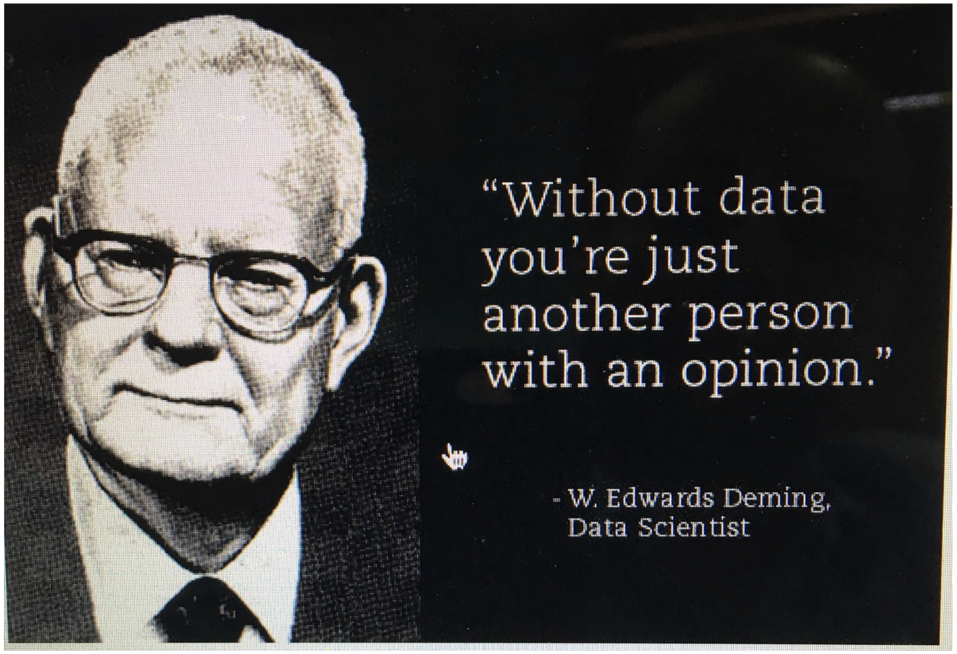
* The data collection was implemented by our **industrial partner**, and *we don't consider it as our contribution in this work.*

Motivation of Measurement Study



"If you can't measure it, you can't improve it."

Peter Drucker



"Without data you're just another person with an opinion."

- W. Edwards Deming, Data Scientist

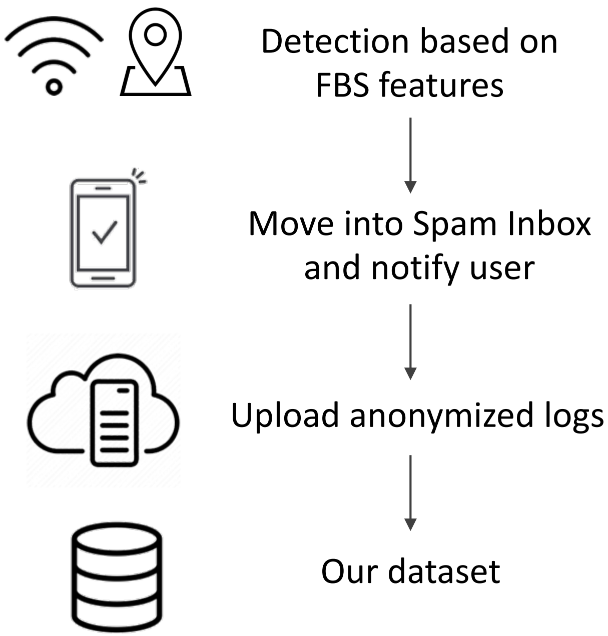
Data Collection (Ethical)

- 279,017 FBS detection logs, Dec.1, 2018 to Mar.7,2019 (97 days)

360
Mobile Guard

Example of Collected Data Logs

2018-12-03 18:43:07	Timestamp (logged time)
95588 (ICBC)	Sender Phone Number
HASH_1	IMEI (hashed for anonymity)
HASH_2	IMSI (hashed for anonymity)
Cellinfo: lac:9418&cellid:3133 2018-12-03 18:43:08,…,…	Information of Recently connected Base Station
157.xxx.xxx.132	IP address of mobile client
您的综合评分良好，可申请提升信用卡额度2万元，www.lcbl95588.com 【工商银行】 With a good overall score, you can apply to increase your credit card limit by ¥20,000. www.lcbl95588.com 【ICBC】	Message Content



Detection based on FBS features

Move into Spam Inbox and notify user

Upload anonymized logs

Our dataset

Research Questions

- Measuring the **Patterns** of FBS Spammers
- Measuring the **Strategies** of Spam Campaigns

- But, **Technical Challenges**

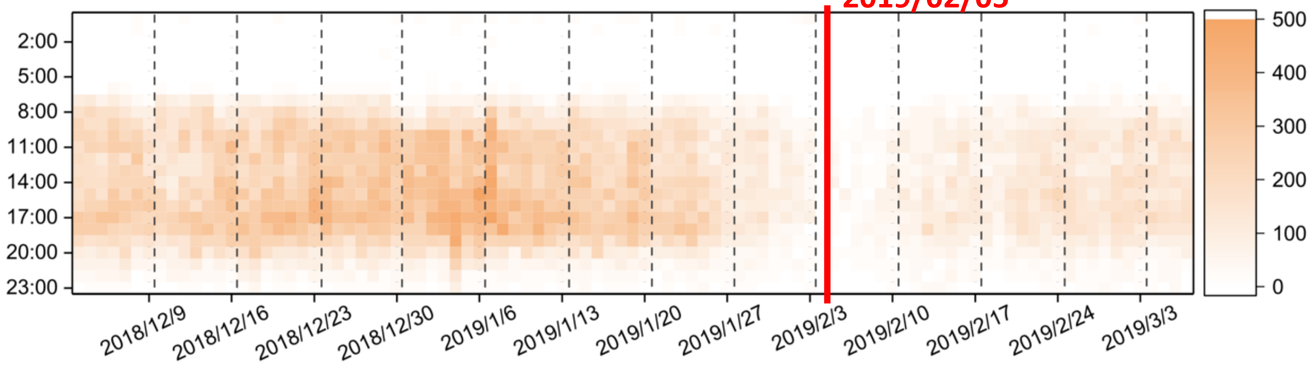
客户，尊敬的范鹏露，恭喜您成为澳门
威尼斯人676fa.com的特邀**會員**，首充
100送128，更有棋牌，电子，**采**票天天
仮点3%哦！。**6WD**

Temporal: Spammers are Hard Working

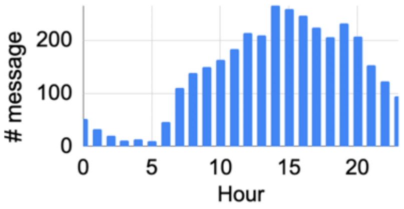
Do spammers keep working on weekends?

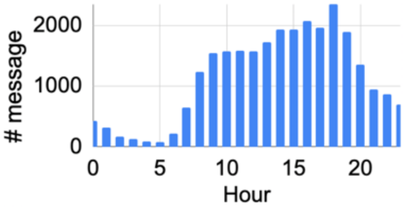
- **Other types of spam**, e.g., domain squatting[ISRAID'17], spam calls[S&P'18]: **No! Take a break!**
- **FBS spam in China ： Yes! Rarely rest.**

Spring Festival
2019/02/05



Heatmap of FBS spam activities

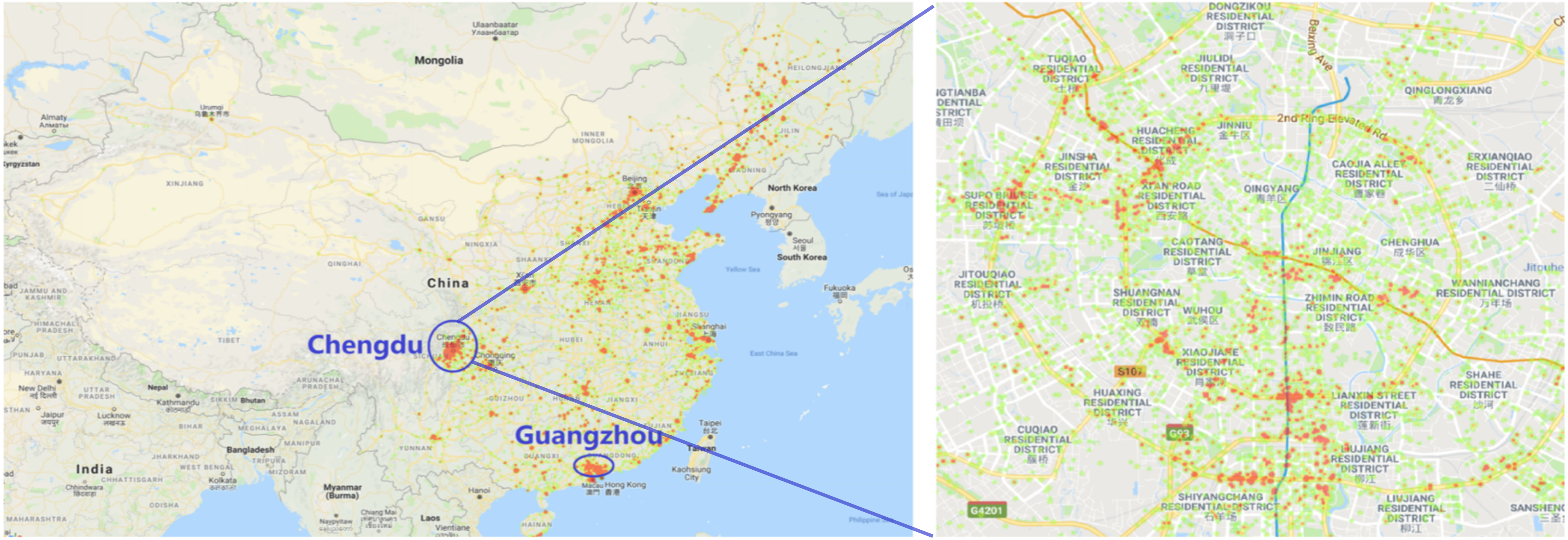




Also keep working after midnight / on New Year's Day.

Only rest around Spring Festival (Gambling spammers remain active then).

Spatial: Crowd Targeted



Largely active near main roads and highly-populated regions for increasing influence

Overview of Spam Campaign

7,884 spam campaigns are identified associated with 8,316 unique spam contacts

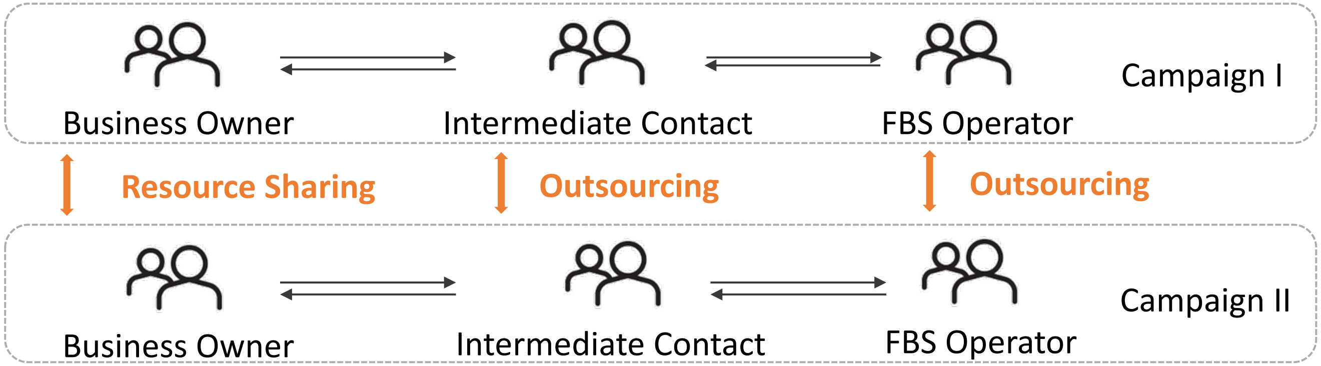
Life time

Mostly short-lived

- 92% active for less than 10 days
- Top 20 **long-lived**: mostly Fake ID and invoice, **"light crime", low risk**
- Top 50 **least-active**: mostly Phishing messages , **"illegal business", high penalty**

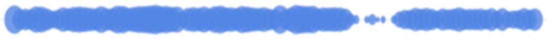
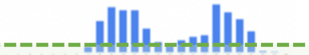
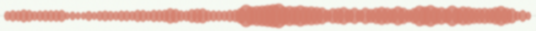
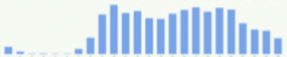
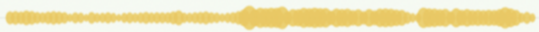
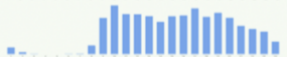
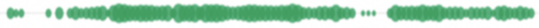
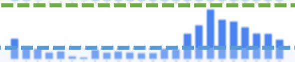
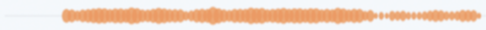
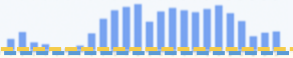
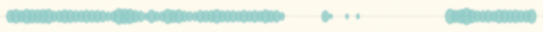
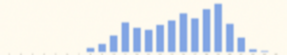
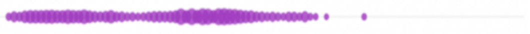
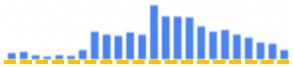
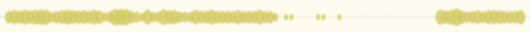
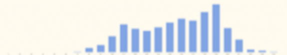
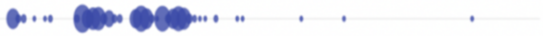
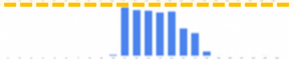
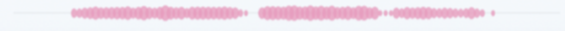
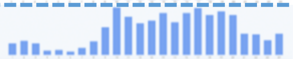
Organization

Hierarchical architecture
Outsourcing models



Overview of Spam Campaign

Top 10 spam campaigns sending most messages

No.	Category	#Msg	#IMEI	Days	Active Time (Dec 1, 2018 – Mar 7, 2019)	Hourly Distribution	Locality
1	Loan	11,120	1,646	95			Dalian
2	Gambling	3,623	2,080	97			Macau
3	Gambling	2,971	1,904	97			Macau
4	Loan	2,327	687	88			Dalian
5	Gambling	1,416	580	77			Macau, Zhuhai
6	Fake ID	1,318	940	71			Chengdu
7	Gambling, Loan, Escort	1,283	460	60			Macau, Zhuhai
8	Ad-Other	1,249	889	72			Chengdu
9	Bank Phishing	1,206	903	35			Cities of Sichuan
10	Gambling	1,127	486	76			Macau, Zhuhai

Outsourcing of FBS Operator

Multiple campaigns could be undertaken of the same FBS operator at the same time

- Campaign 2&3, 5&10, 6&8 are similar both in active time and active location, with at least 54% overlap of affected IMEIs

Evasion Strategies of Spam Campaigns

Domain Infrastructure

Newly registered domains

1,155 (38.4%) domains are registered after 2019

Domain-squatting services

278 are over 3 years old registered early, leveraged in batches

URL-shorten

397 (69%) URLs use *URL shorteners*

http://t.cn/xxxxxx *http://dwz.cn/xxxxx*

-> Avoid Domain Blacklisting

Bank Account

Abusing flawed bank policy

Registered in mid-west China with flawed bank policy

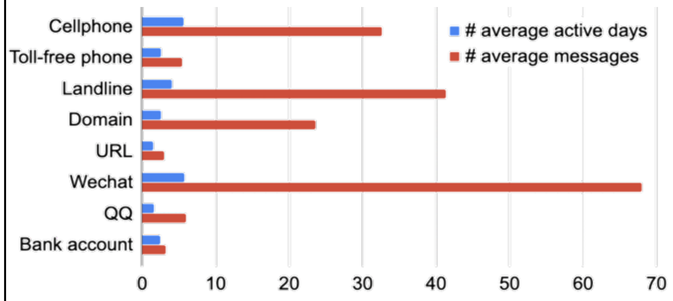
Loose Authentication

Free Secondary Card

-> Avoid Bank Blocking

Spammer Contacts

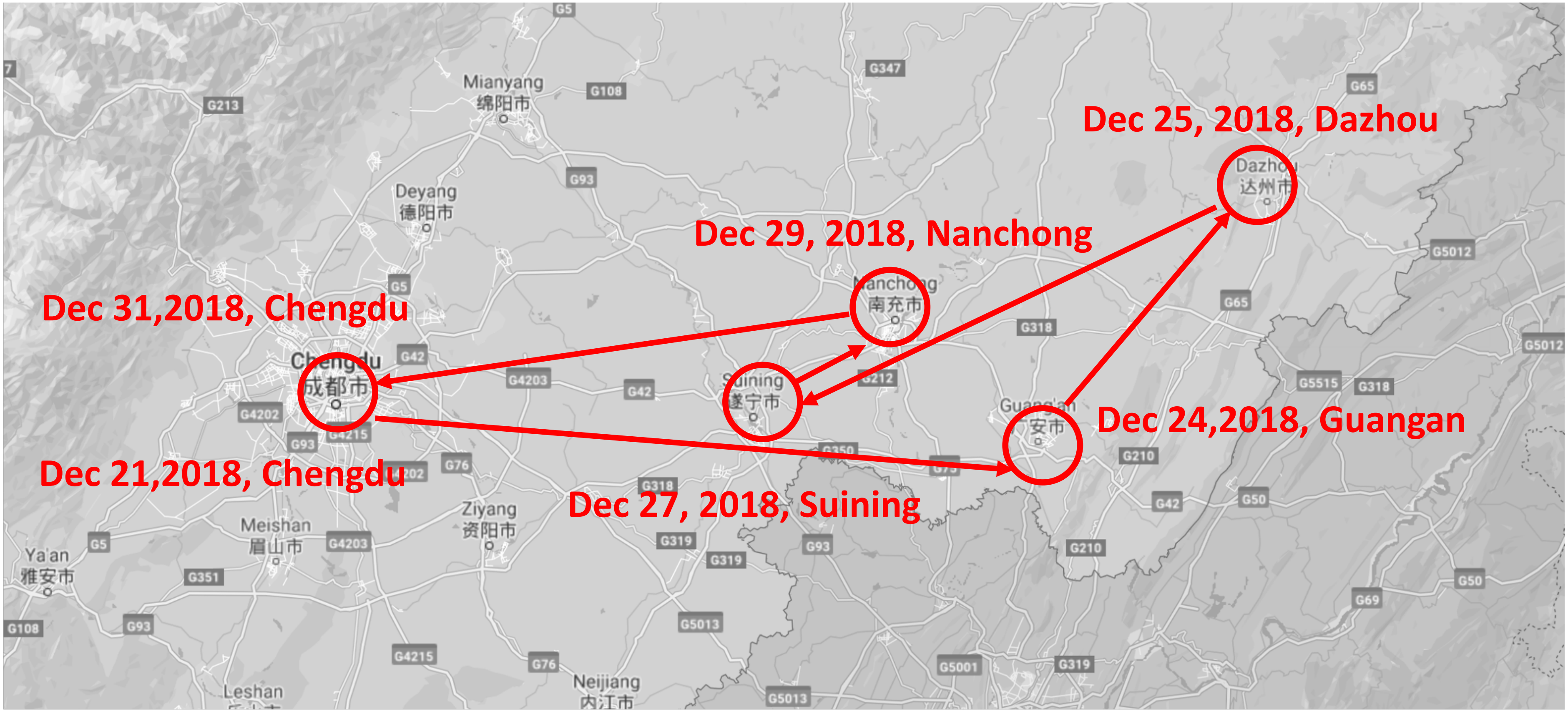
Social platform accounts for the most



Low blocking rate, long live-time

-> Avoid Account Blocking

Moving Spam Campaign



Dec 25, 2018, Dazhou

Dec 29, 2018, Nanchong

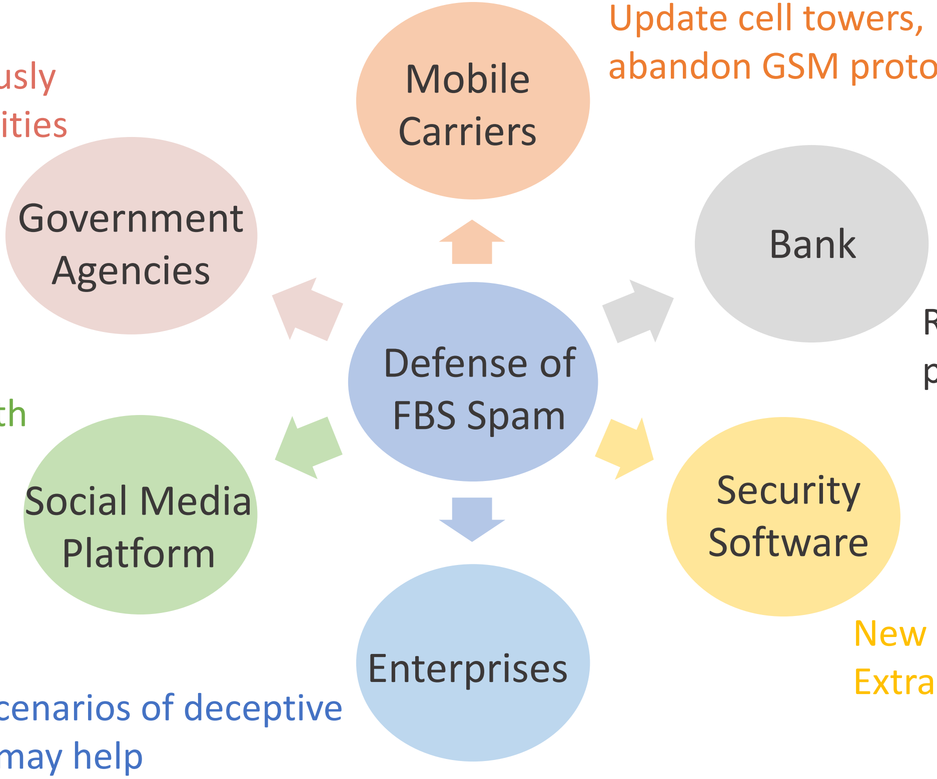
Dec 31,2018, Chengdu

Dec 24,2018, Guangan

Dec 21,2018, Chengdu

Dec 27, 2018, Suining

Recommendations for the Community



Update cell towers, abandon GSM protocol

More efforts in seriously effected places and cities

Re-evaluate their bankcard policies to avoid being abused

Checking accounts with fraudulent activities

New UI system of application
Extracted templates as new features

User education, new scenarios of deceptive messages in our work may help

All of the parties evolved in FBS Ecosystem should unite and work together to mitigate FBS Spam issues.

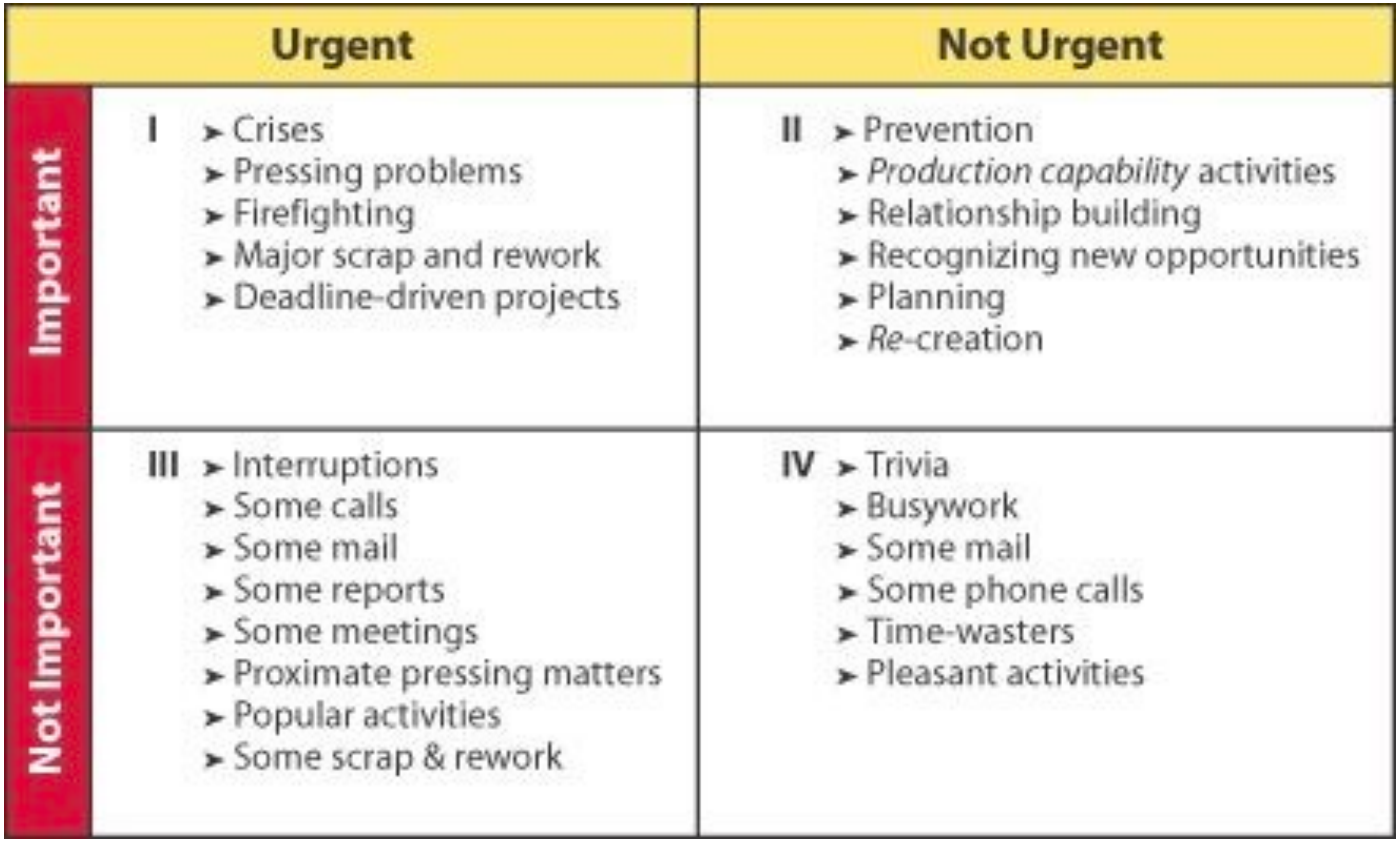
1. Common Sense

2. Case Studies

3. **Some Tips**

管好自己

规划时间，以投资的角度对待时间分配



	Urgent	Not Urgent
Important	I ➤ Crises ➤ Pressing problems ➤ Firefighting ➤ Major scrap and rework ➤ Deadline-driven projects	II ➤ Prevention ➤ *Production capability* activities ➤ Relationship building ➤ Recognizing new opportunities ➤ Planning ➤ *Re*-creation
Not Important	III ➤ Interruptions ➤ Some calls ➤ Some mail ➤ Some reports ➤ Some meetings ➤ Proximate pressing matters ➤ Popular activities ➤ Some scrap & rework	IV ➤ Trivia ➤ Busywork ➤ Some mail ➤ Some phone calls ➤ Time-wasters ➤ Pleasant activities

受限条件下的优化问题

避免完美主义

The closer you look, the less you will see.
Now you see me.

广泛合作

“管”好导师

照顾好身体和情绪

Q & A

- Location: FIT 4-204
- Email: lbj@mail.tsinghua.edu.cn

刘保君

中国大陆