Anti-Spam Technologies and Operation

Kazu Yamamoto
Internet Initiative Japan, Inc.
kazu@iij.ad.jp

Cellular Phones

- Japan is a paradise of cellular phones
  - About 70% of Japanese have them
- They provide e-mail services
  - AU, DoCoMo, and Vodafone

Spammers' gear

宣伝メール配信にもっとも強力な新製品が出ました！！

携帯による携帯メール自動送信システム発売！！

ドメイン指定拒否されていても届きます。(悪用厳禁！)

AU by KDDI(CDMA)携帯電話1〜20台接続型
通常価格2,300,000円を 特別価格898,000円
内容:送信システムインストール済PC1本体(モニタ別)+携帯接続ケーブル10本(追加ケーブル1本3980円)

AU by KDDI(CDMA)携帯電話1〜5台接続型
通常価格1,800,000円を 特別価格498,000円
内容:送信システムインストール済PC1本体(モニタ別)、携帯接続ケーブル5本¥50000別売)

※お届けは入金後1~2週間程度になります。
他社AUシステムよりかなり安くて最も高速なメール配信システム！ ここでしか買えません！！
お電話はいますぐ！ 0909-5656-588 へどうぞ！！
メールなら info@hitbitweb.com
New! パケット定額WIN端末対応型完成！↓

- Some spammers pay much cellular phone fee
- But they earn more

Spam Tendency

- Spams to cellular phones is decreasing
  - Rate control by the carriers
  - Canceling contract of spammers
    - The carriers can identify users
- Spams to PCs is drastically increasing
  - 10 times larger in Aug 2004
  - Due to "Zombie" clusters or "Botnets"
  - Mail addresses can be faked

Categories of Spam

- Unsolicited advertisement (**未承諾広告**)
- Phishing
  - Japanese versions appeared
- Trap to online dating (**出会い系サイトへの誘導**)
  - Starting with daily conversation
  - Continuing conversation leads the victim to an online dating system
  - He will result in paying much money

Trap to online dating

- Do you want to reply to this?

  Subject: Excuse me.
  From: Tomomi INOUE

  You sent me a message, didn't you?
  I thought this is a spam at first
  but I realized that your address does not seem strange.
  So, I'm replying to you.
  Are you a guy with whom I had a chat on the net??

  Subject: **あの～**
  From: **井上知美**

  メールくれましたよね？
  最初は迷惑メールかと思ってたんだけど
  よく見たらそんな変なアドレスじゃないので
  メール返してみたんですが、
  以前どちらかのチャットか何かでお話したかたですか？？

- It is very difficult to filter this kind of spams!

Phishing Message

UFJ銀行　こたえていくチカラ。

UFJ銀行ご利用のお客様へ

UFJ銀行のご利用ありがとうございます。
このお知らせは、UFJ銀行をご利用のお客様に発送しております。

この度、UFJ銀行のセキュリティーの向上に伴いまして、
オンライン上でのご本人確認が必要となります。

この手続きを怠ると今後のオンライン上での操作に支障をきたす恐れがありますので、一刻も素早いお手続きをお願いします。

https://www.ufjbank.co.jp/ib/login/index.html

また、今回のアップデートには多数のお客様からのアクセスが予想されサーバーに負荷がかかるため、下記のミラーサイトを用意しております。上記のリンクが一時期不可能になっている場合は、下記をご利用ください。

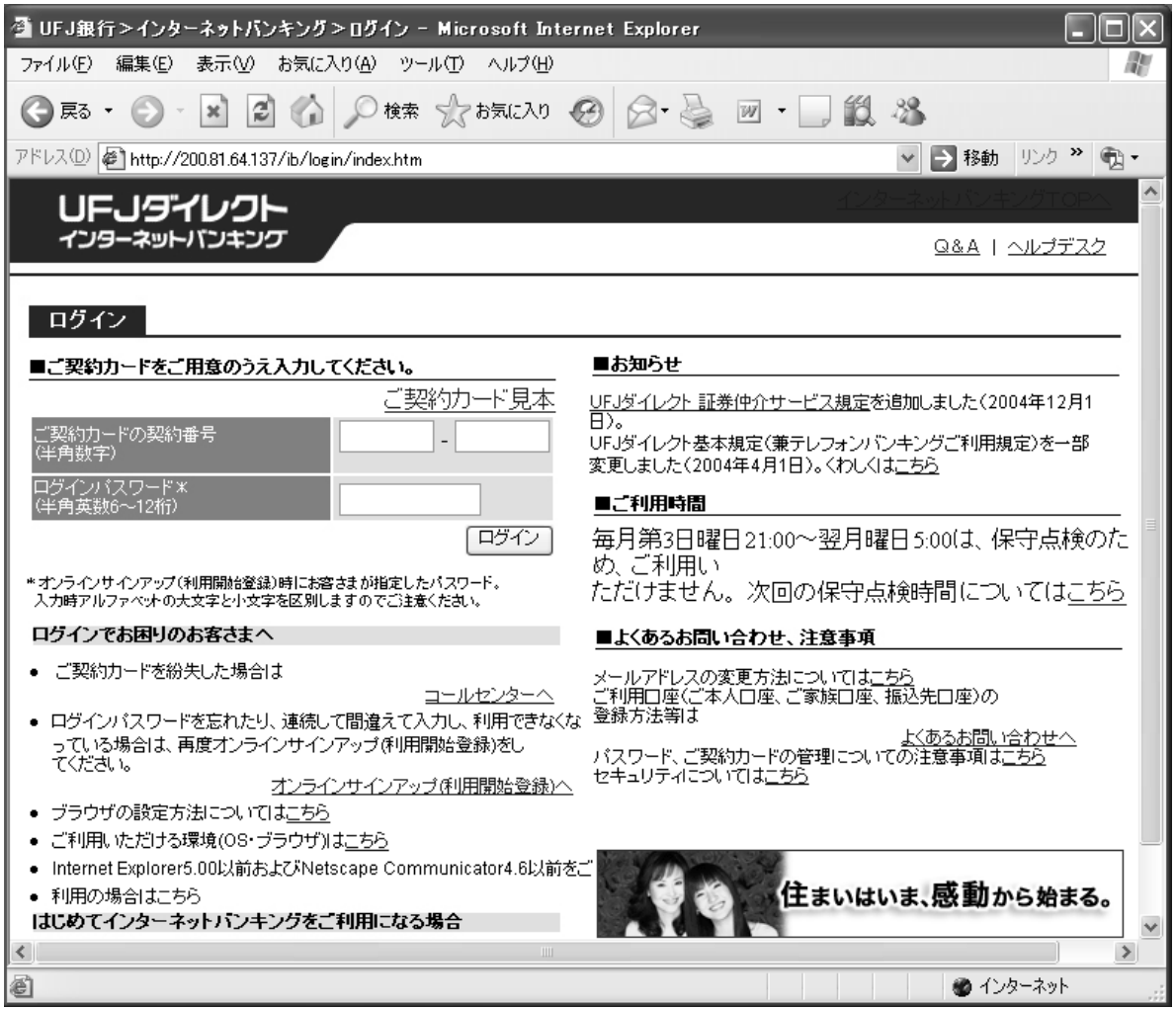
https://www.ufjbank.co.jp/ib/login/index2.html

https://www.ufjbank.co.jp/ib/login/index3.html

お客様のご協力とご理解をお願いいたします。

UFJ銀行

Phishing Site



Phising Page

Statistics

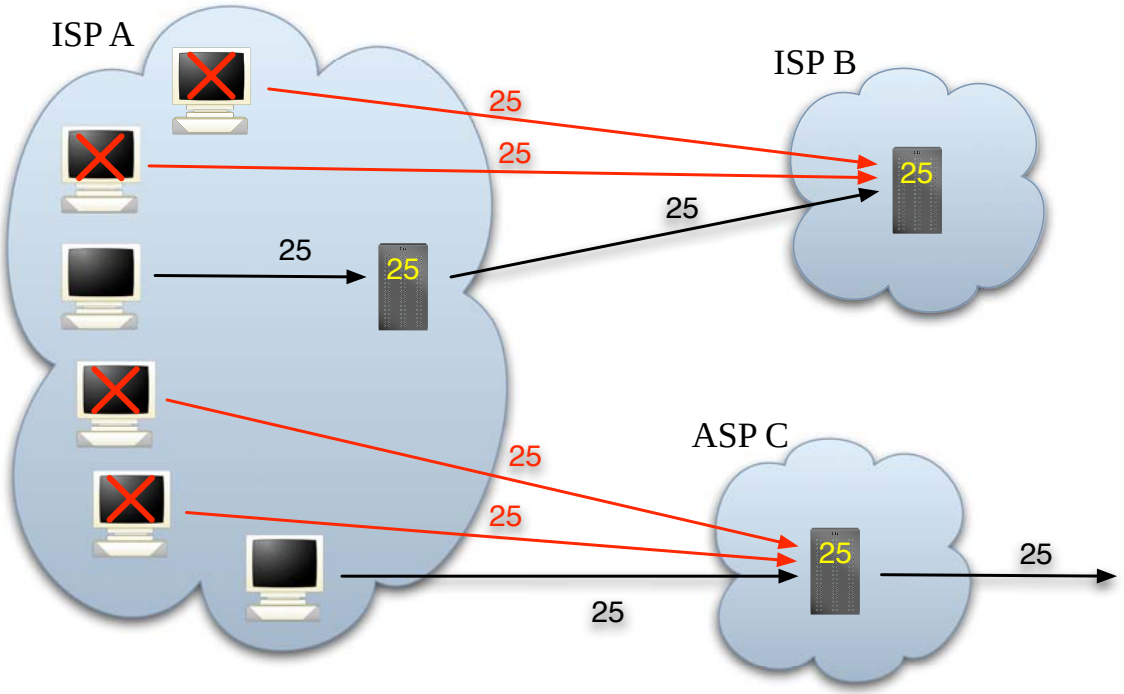
- Where do spams come from?
  - IIJ counted "user unknown" messages
  - Resolving a country with its source IP address
  - 2004.12.20

total 374,093

JP 99,370 (26.6%)
US 83,287 (22.3%)
KR 63,097 (16.9%)
CN 40,791 (10.9%)
FR 8,437 (2.3%)

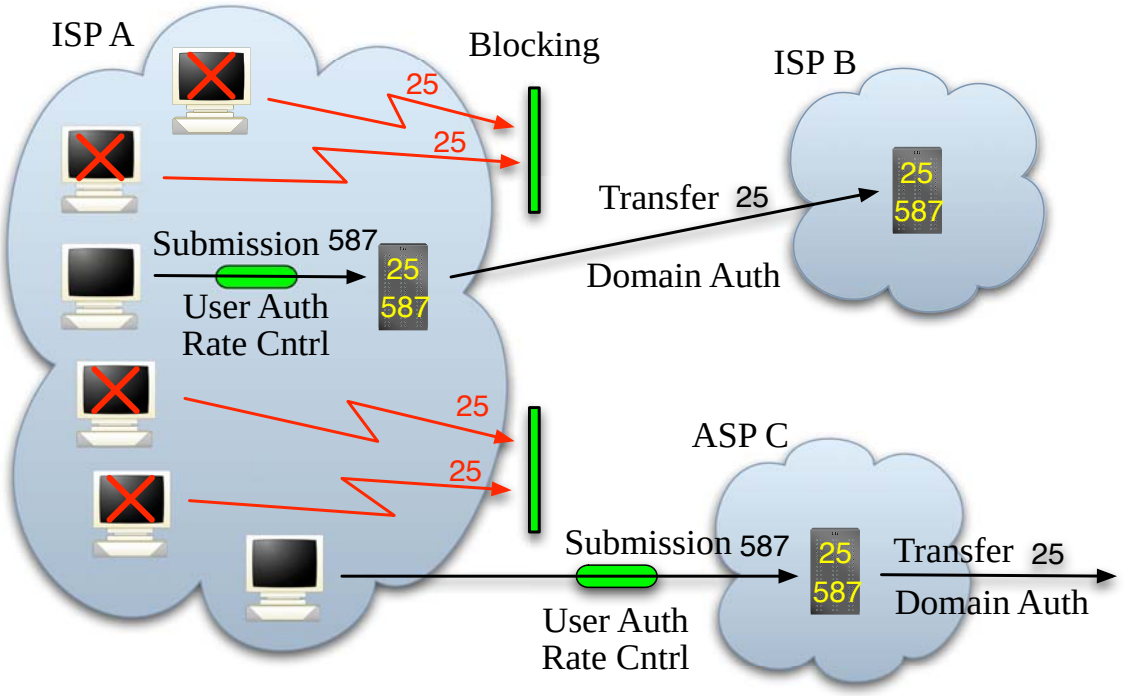
- We should recognize JP, KR & CN generate many spams!
  - We need to collaborate to decrease spams
  - Otherwise, the entire AP region would be filtered out by other regions

Current



- Massive spams from Zombies
- Phishing with faked e-mail addresses

Near Future



- Separation of transfer and submission
- Blocking spams from Zombies
- Submission with user authentication
- Transfer with domain authentication

Measurement of Domain Auth

- How many domains support domain auth?
  - Joint research of the WIDE project and JPRS
  - Measuring RRs of domains under ".jp"

Zone	total	MX	SPF	DK
JP	397161	255087	489	1
AC	3192	3003	10	0
AD	299	257	10	1
CO	275219	255199	236	3
ED	4327	3916	0	0
GO	839	722	1	0
GR	9149	7762	14	0
LG	2673	982	0	0
NE	17299	13178	68	1
OR	20352	18971	20	1
GEO	4010	3445	8	0
Total	734520	562522	856	7