

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(モニター別)+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(モニター別)、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も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



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

UFJ銀行 > インターネットバンキング > ログイン - Microsoft Internet Explorer

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り

アドレス http://200.81.64.137/ib/login/index.htm

UFJダイレクト インターネットバンキング

Q&A | ヘルプデスク

ログイン

■ご契約カードをご用意のうえ入力してください。

ご契約カード見本

ご契約カードの契約番号 (半角数字)	<input type="text"/> - <input type="text"/>
ログインパスワード* (半角英数6~12桁)	<input type="password"/>

*オンラインサインアップ(利用開始登録)時にお客さまが指定したパスワード。
入力時アルファベットの太文字と小文字を区別しますのでご注意ください。

■お知らせ

UFJダイレクト 証券仲介サービス規定を追加しました(2004年12月1日)。
UFJダイレクト基本規定(兼テレホンバンキングご利用規定)を一部変更しました(2004年4月1日)。くわしくはこちら

■ご利用時間

毎月第3日曜日 21:00~翌月曜日 5:00(は、保守点検のため、ご利用いただけません。次回の保守点検時間についてはこちら)

■よくあるお問い合わせ、注意事項

メールアドレスの変更方法についてはこちら
ご利用口座(ご本人口座、ご家族口座、振込先口座)の登録方法等は
パスワード、ご契約カードの管理についての注意事項はこちら
セキュリティについてはこちら

よくあるお問い合わせへ
こちら

ログインでお困りのお客さまへ

- ご契約カードを紛失した場合は
[コールセンターへ](#)
- ログインパスワードを忘れたり、連続して間違えて入力し、利用できなくなっている場合は、再度オンラインサインアップ(利用開始登録)をしてください。
[オンラインサインアップ\(利用開始登録\)へ](#)
- ブラウザの設定方法については[こちら](#)
- ご利用いただける環境(OS・ブラウザ)は[こちら](#)
- Internet Explorer5.00以前およびNetscape Communicator4.6以前をご利用の場合は[こちら](#)

はじめてインターネットバンキングをご利用になる場合

住まいはいま、感動から始まる。

Phising Page

UFJ - 最新情報 - Microsoft Internet Explorer - [オフライン作業]

ファイル(E) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 進む 印刷 検索 お気に入り メディア

アドレス http://61.38.30.55/ib/login/update.htm 移動 リンク

Google ウェブ検索 サイト検索 オプション

UFJダイレクト インターネットバンキング

最新情報

姓

名

ご契約カードの契約番号 -

ログインパスワード*

クレジットカード番号

有効期限 Month Year

桁の暗証番号

(C) Copyright 2005, UFJ Bank Limited  UFJ銀行

Statistics

- Where do spams come from?
 - IJ 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%)

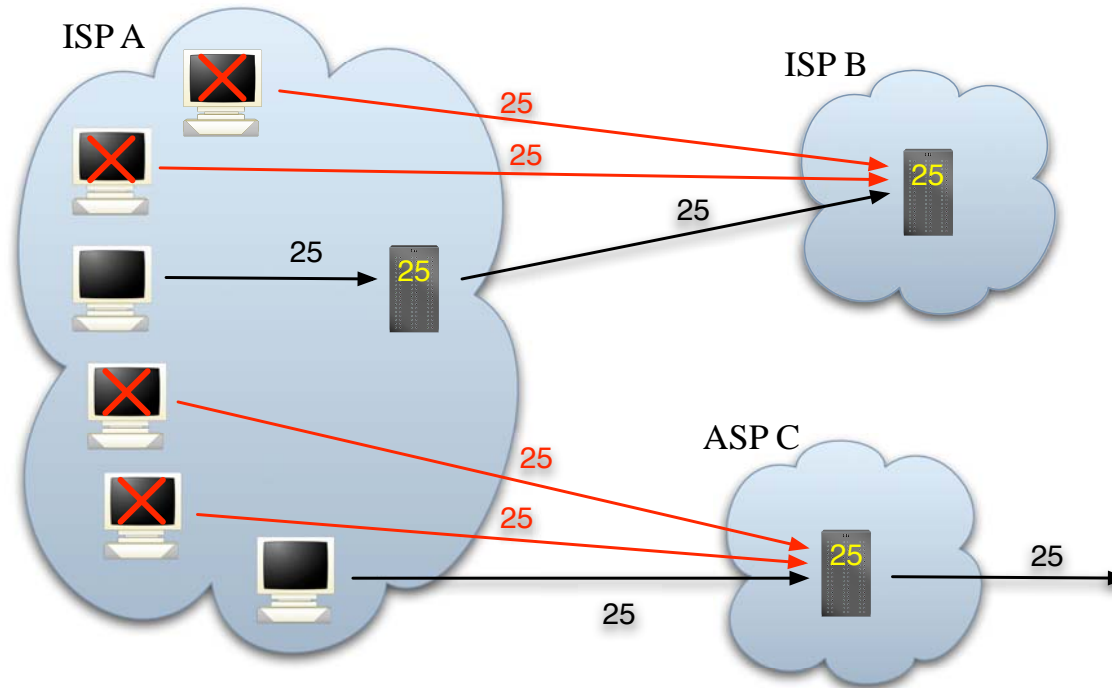
KR 63,097 (16.9%)

CN 40,791 (10.9%)

FR 8,437 (2.3%)

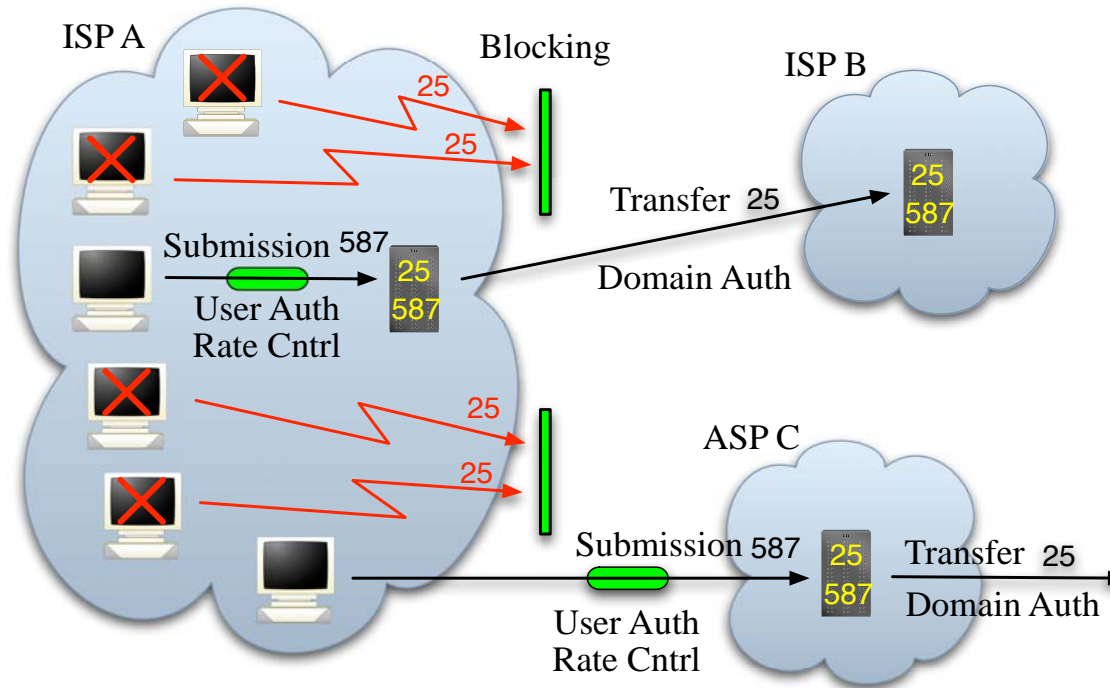
- We should recognize JP, KR & CN generate many spams!
 - We need to collaborate to decrease spams
 - Otherwise, the entire AP region would be filtered out by other regions

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