



IBM Research

Breaking Anti-Spam Systems with Parasitic Spam

[Morton Swimmer](mailto:Morton_Swimmer@acm.org) swimmer@acm.org

[Barry Leiba](mailto:Barry_Leiba@watson.ibm.com) leiba@watson.ibm.com

[Ian Whalley](mailto:Ian_Whalley@us.ibm.com) inw@us.ibm.com

[Nathaniel Borenstein](mailto:Nathaniel_Borenstein@us.ibm.com) nborenst@us.ibm.com

July 27, 2006

© 2006 IBM Corporation

Problem statement – Parasitic Spam

- **Zombie networks**
 - Zombie: a Trojan horse used to send spam
 - Set up and run by spammers
 - Account for huge quantities of spam
 - Distribute the CPU and bandwidth required

- **But once zombies exist they could be used for something more insidious**
 - A zombie may intercept email in transit
 - Then, add spam to this email
 - The zombie could be on user workstation
 - ... or on any other part of the email infrastructure

- **Problem: the email is legitimate, but still contains unwanted content**

Mechanics of P-Spam

Alice writes email

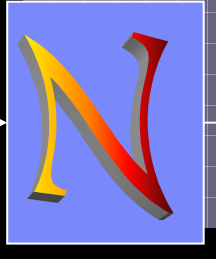
- **Example:**
 1. Alice writes an email to Bob
 2. The zombie intercepts the outgoing email
 3. Adds the spam to it as a “signature”
 4. The P-Spam is delivered to Bob
- **Note:**
 - Both sender and recipient are legitimate
 - The email contains both ham and spam

```
From: Alice
To: Bob
Subject: Good to hear
        from you again

We should chat more
often, Bob.

Cheers, Alice
```

(this is the email
that Alice wrote)



(The zombie
modifies the
email)

```
From: Alice
To: Bob
Subject: Good to hear
        from you again

We should chat more
often, Bob.

Cheers, Alice
--
Buy your physical
enhancements at:
http://spamm.er
```

(this is the email
that is delivered)

Email
delivery

What P-spam looks like

- P-Spam may take any number of forms, for example:
 - An added signature
 - A new multipart/* section
 - Add or modify existing text
- Each has a different degree of intrusiveness
- Each offers different problems for removal

```
From: Alice
To: Bob
Subject: Good to hear from you again

We should chat more often, Bob.

Cheers, Alice
--
Check out: http://spamm.er for your physical
enhancements.
```

```
From: Alice
To: Bob
Subject: Good to hear from you again
Content-Type: multipart/mixed;
boundary="break"
--break
Content-Type: text/plain
We should chat more often, Bob.

Cheers, Alice
--break
Content-Type: text/plain
Check out: http://spamm.er for your physical
enhancements.
--break--
```

```
From: Alice
To: Bob
Subject: Good to hear from you again

We should chat more often, Bob.

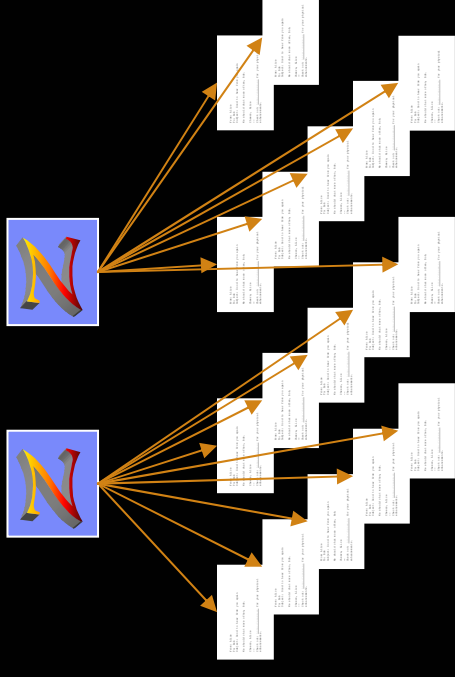
Check out: http://spamm.er for your physical
enhancements.

Cheers, Alice
```

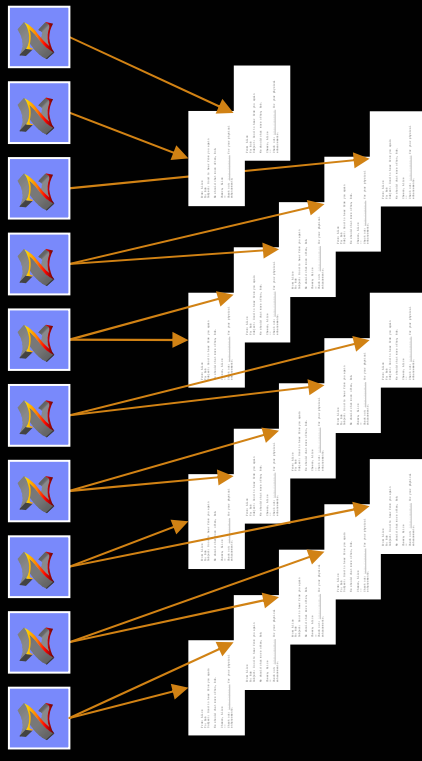
How likely is P-Spam?

- Little motivation at the moment
 - Mass spamming provides good ROI
 - New spam techniques still foil anti-spam tools for a while
 - Short massive campaign more appealing than protracted campaign
 - Fairly small numbers of zombies are needed
- However, Spammers will adapt if anti-spam tools get better
 - They will require larger zombie networks
 - They will need code for hooking the email delivery stack
 - They will need more time to get the message out
- But, P-Spam cannot be blocked: better hit rate

(few zombies each send massive amounts of spam)



(many zombies each send small amounts of spam)

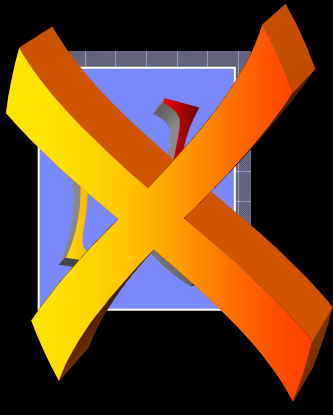


Countermeasures

- MUA/MUA and Server/Server authentication will not help
 - The email is legitimate
 - It passes through all legitimate channels
- Danger: P-Spam may look either spam or ham
 - If scores spam, then email is not delivered: false positive!
 - If scores ham, then spam is delivered: annoyance or danger to user
- Therefore
 - Anti-spam tools need to classify by email region
 - And remove spam regions before delivery
- Single most effective solution: *Get rid of the zombies!*
 - Integrate anti-spam solutions with intrusion detection systems and vulnerability scanners

Conclusions

- Intension: make this a non-issue
 - Products can be modified now
 - To handle spam in ham
 - To filter out the spam before delivery
 - More work done to combat zombies
- Raise awareness of the problem
 - Are false positives and negatives really P-Spam?
- Then, P-Spam will never become attractive and we have one problem less



Questions?