

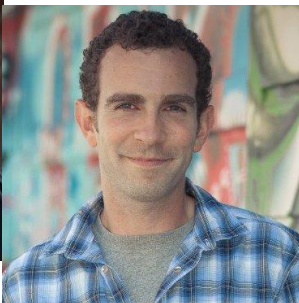
SREcon 15

03.16.15-03.17.15 | SANTA CLARA, CA



The Weeping Angels of Site Reliability

Tuesday 2015-03-17 11:30-12:30





Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection
- 3) Bad Content
- 4) Intra-service Attacks
- 5) Outbound Abuse
- 6) Third Party Compromise



Why DMARC?

GROUPON


Hi there!

You're going to love it


We are glad to inform you that one of your friends has found a great deal on Groupon.com!
And even shared it with you!

Yeah! Now **Groupon.com** gives an opportunity to share a discount gift with a friend!
Enjoy your discount gift in the attachment and share it with one of your friend as well.

All the details in the file attached. be in a hurry this weekend special is due in 2 days!

 **The Groupon Promise**


The Groupon Promise. We got your back!
If the experience using your Groupon ever lets you down, we'll make it right or return your purchase.
Simple as that.

 **Take us with you**
Download the mobile app to keep Groupon in your pocket or purse.

Need help? [Contact Groupon](#)

Delivered by Groupon Inc. 600 W. Chicago Avenue, Suite 620 Chicago, IL 60654, USA

You are receiving this email because you signed up for the Daily Groupon alerts. If you prefer not to receive the daily Groupon email, you can always unsubscribe with [one click](#) or manage your [subscriptions](#). Be sure to add us to your address book or safe sender list so our emails get to your inbox. [Learn how](#)



GROUPON


Thanks for Joining!

You're going to love it


Check your inbox every day to discover Groupon deals with huge discounts on tasty meals, relaxing spa days, concerts, 5-star hotels and more.

Get better deals. Take a second to tell us a bit about yourself.

Personalize Your Deals

 **The Groupon Promise**


The Groupon Promise. We got your back!
If the experience using your Groupon ever lets you down, we'll make it right or return your purchase.
Simple as that.

 **Take us with you**
Download the mobile app to keep Groupon in your pocket or purse.

Need help? [Contact Groupon](#)

Delivered by Groupon Inc. 600 W. Chicago Avenue, Suite 400 Chicago, IL, 60654, USA

You are receiving this email because you signed up for the Daily Groupon alerts. If you prefer not to receive the daily Groupon email, you can always manage your subscriptions. Be sure to add us to your address book or safe sender list so our emails get to your inbox. [Learn how](#)





GROUPOONTM

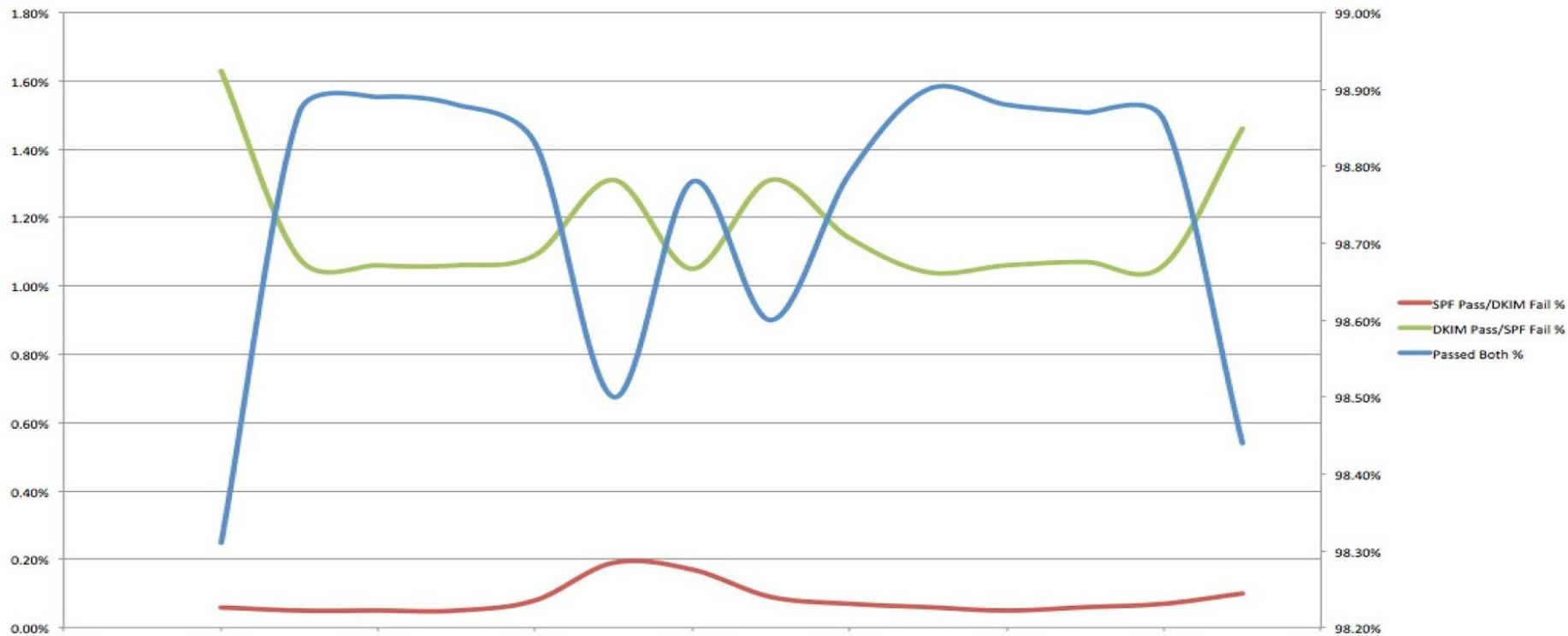
Collective Business

Fake Groupon discount emails carry malware

Cybercriminals have spammed out malware, attached to emails claiming to be related to discounts for offers on Groupon. The emails, which have the poorly spelt subject line of "Groupon dicount gifts" (in itself something which should ring alarm bells), pretend to come from Groupon, and claim that one of your friends has found a deal on the website.

<https://nakedsecurity.sophos.com/2012/07/30/fake-groupon-email-malware/>

The Data



Blocked

Seu Groupon diário em Shopping | Adicione "noreply@groupon.com.br" aos seus endereços de e-mail.

Clique aqui para gerenciar as mensagens que recebe do Groupon, ou cancele o recebimento do e-mail Shopping com um clique.

GROUPON Suas ofertas de hoje de Shopping

Apple iPhone 5
Mais de 200 comprados
Apple iPhone 5 16GB de R\$ 2.799,00 por R\$ 599,00. Exklusividade Groupon
Frete grátis... mais.

PlayStation 4


Veja a oferta R\$ 2.799,00 **R\$ 599,00**

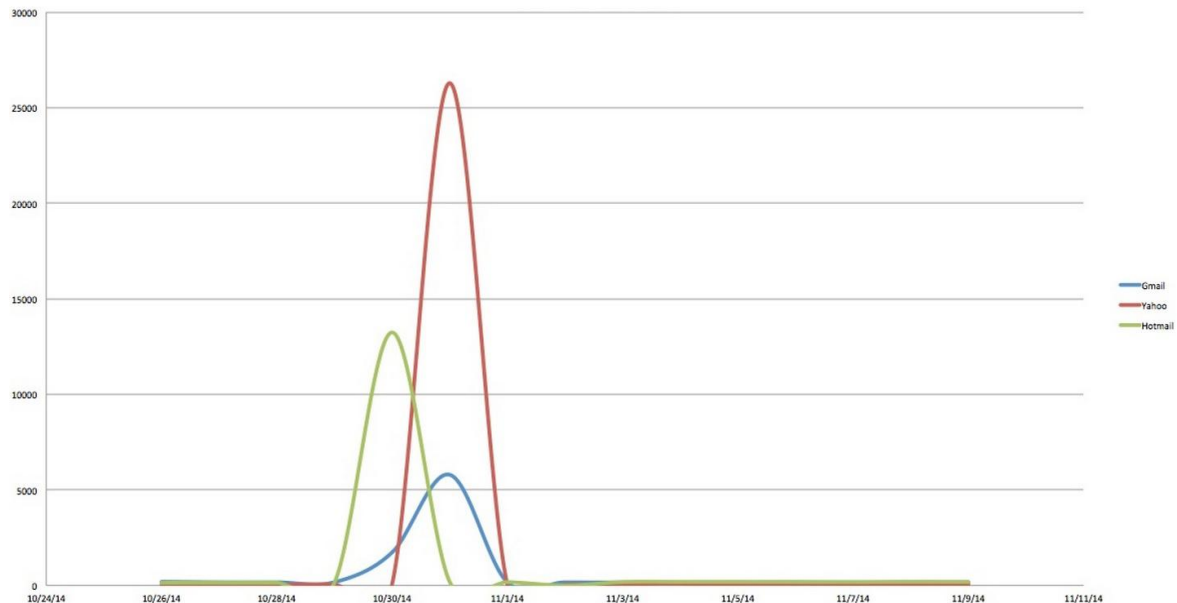
TRAMONTINA
VER OFERTAS >

Photobook Luxo Natal
R\$ 74,00 **R\$ 28,90** [Veja](#)

Colchão Ortobom Physical Spring Black
Mais de 200 comprados
R\$ 379,00 [Veja](#)

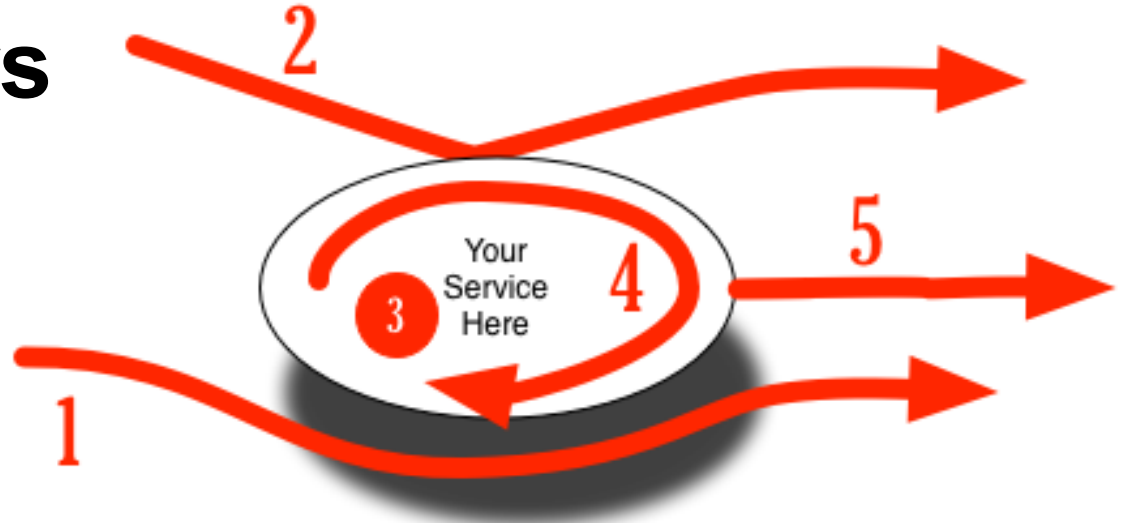
Centrum





Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection**
- 3) Bad Content
- 4) Intra-service Attacks
- 5) Outbound Abuse
- 6) Third Party Compromise



Amplification/Reflection Attacks

- Open[SMTP|DNS|NTP|other] reflection
 - <http://openNTPproject.org/>
 - <http://openRESOLVERproject.org/>
 - [ISOC Amplification Hell](#)
- Spoofed traffic bounce “back” against victims

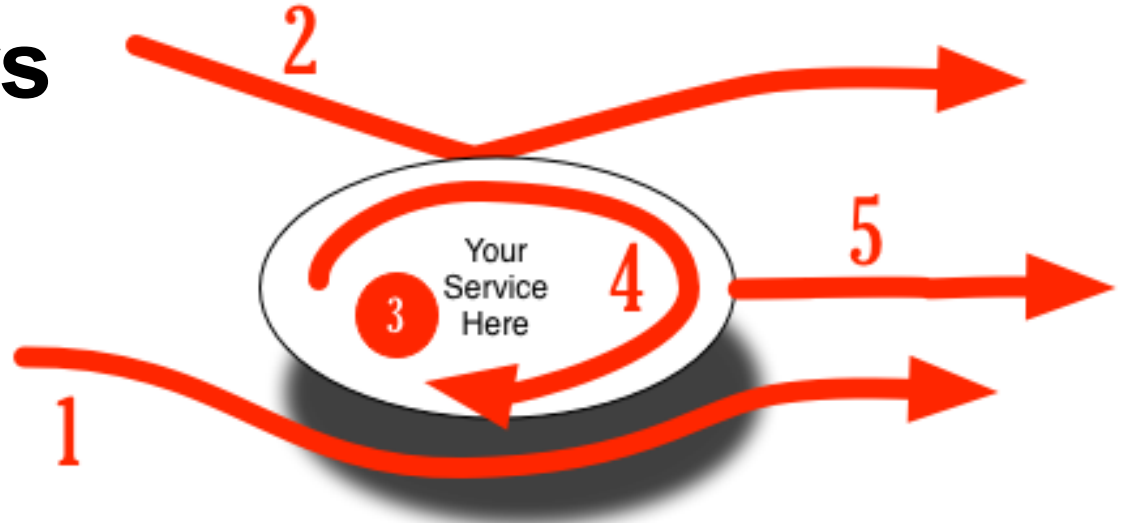


Can your service be an oracle?



Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection
- 3) **Bad Content**
- 4) Intra-service Attacks
- 5) Outbound Abuse
- 6) Third Party Compromise



Anti-Abuse Cloud Best Practices



Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection
- 3) Bad Content
- 4) Intra-service Attacks**
- 5) Outbound Abuse
- 6) Third Party Compromise

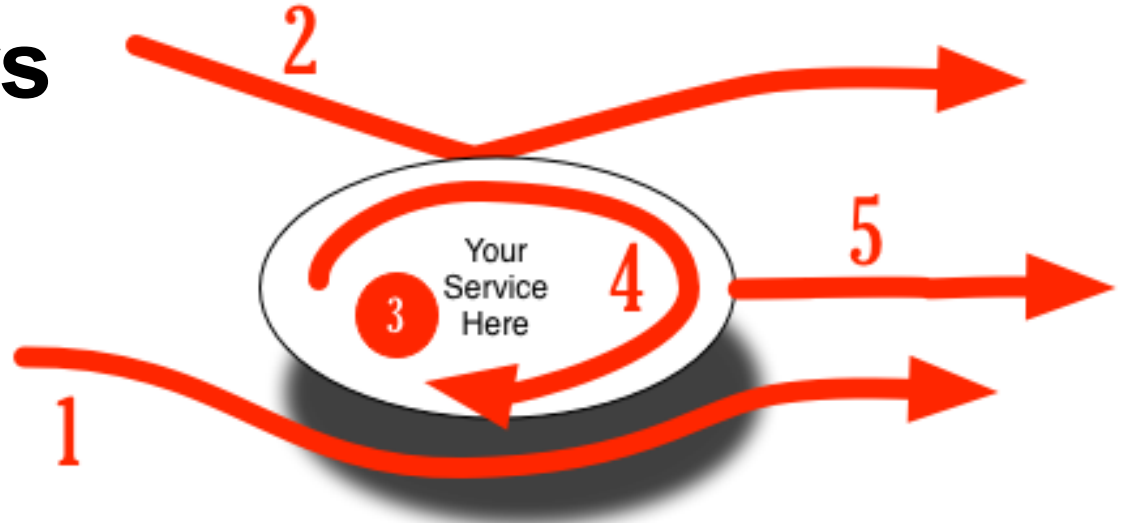


Intra-service defenses

- Protect credentials
- Watch tunnels / weak endpoint-security
- Watch out for unauthenticated connections
- Logs can be your friend, but also your enemy

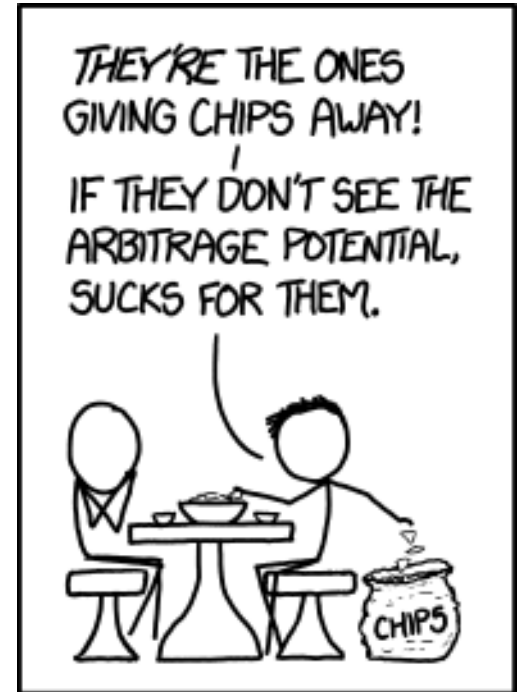
Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection
- 3) Bad Content
- 4) Intra-service Attacks
- 5) Outbound Abuse**
- 6) Third Party Compromise



If you build it. . .

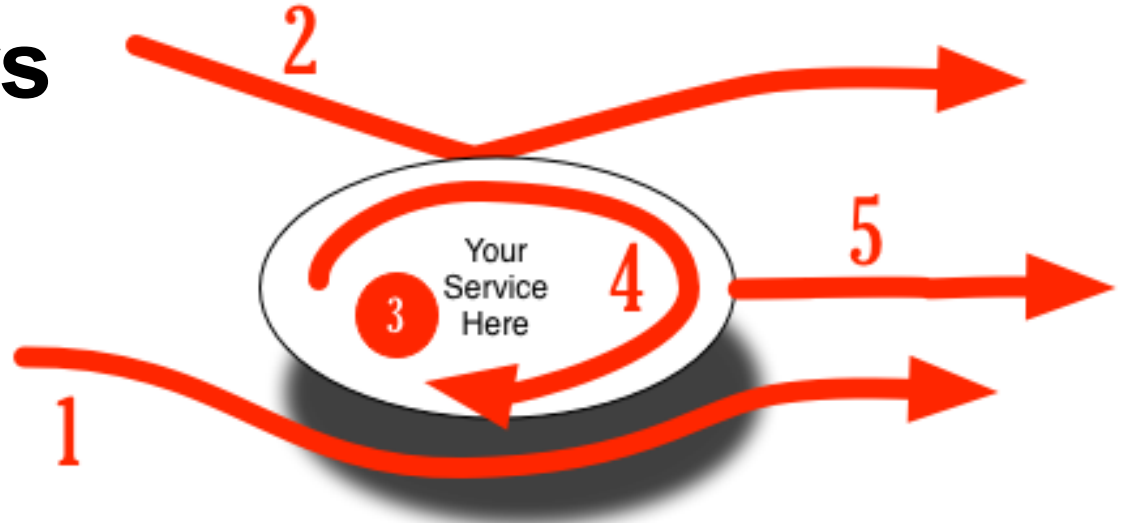
. . .it will be abused.



IN A DEEP SENSE, SOCIETY FUNCTIONS ONLY BECAUSE WE GENERALLY AVOID TAKING THESE PEOPLE OUT TO DINNER.

Abuse Vectors

- 1) Shadow or Reputational
- 2) Reflection
- 3) Bad Content
- 4) Intra-service Attacks
- 5) Outbound Abuse
- 6) **Third Party Compromise**



Third-party services: Common issues

Examples: Source code repositories, monitoring, crash analytics, user analytics

- Account provisioning and permissioning
- Authentication and account recovery
- Excessive sharing of user data or sensitive info
- Lack of sufficient audit trails

Another take on third parties



Take-away points

1. Get paranoid about any social/communications features
2. Limit payloads; do you really need a custom message including arbitrary links?
 - a. Beware of all user-generated content (UGC)
3. Rate limits, quotas, and metrics
4. ~~Trust but~~ verify, verify, verify
5. Encrypt everything, everywhere, all the time (in motion and at rest)
6. Be mindful of how international users utilize your platform
7. Both users and attackers will use/abuse your platforms in ways you would never expect

