SOCIAL MEDIA DECEPTION

Aamir Lakhani @aamirlakhani

World Wide Technology

Joseph Muniz

Cisco System

RSACONFERENCE
EUROPE 2013

Session ID: HUM-W01

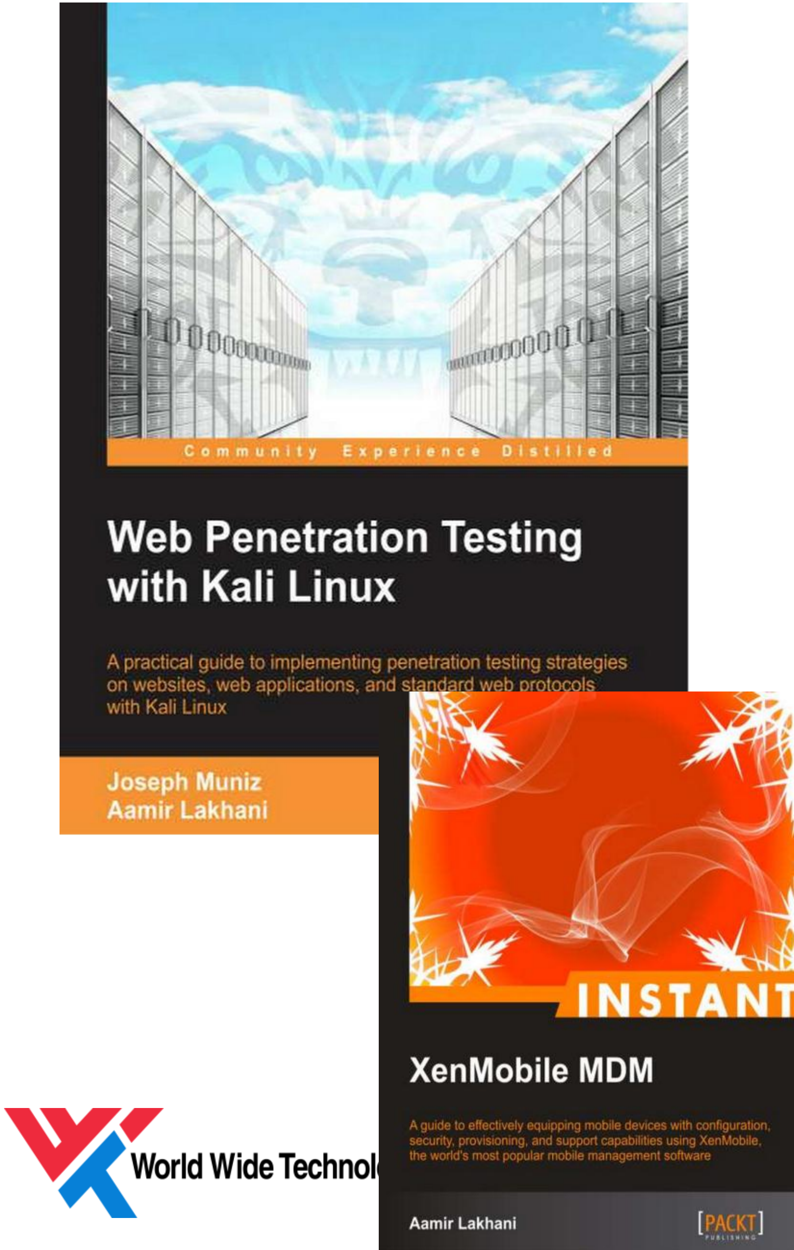
Session Classification: Intermediate

Contact Information

- Aamir Lakhani – aka Dr. Chaos
  - Blog: www.DrChaos.com
  - Twitter: @aamirlakhani
  - Senior Counter Intelligence and Cyber Defense specialist

- Joseph Muniz – aka The Security Blogger
  - Blog: www.TheSecurityBlogger.com
  - Senior Cyber Defense Solutions Architect

- Presentation on our blogs: Search for RSA Europe



Community Experience Distilled

Web Penetration Testing with Kali Linux

A practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux

Joseph Muniz
Aamir Lakhani

INSTANT

XenMobile MDM

A guide to effectively equipping mobile devices with configuration, security, provisioning, and support capabilities using XenMobile, the world's most popular mobile management software

Aamir Lakhani

[PACKT] PUBLISHING

Have You Ever Told A Lie?

- People believe white lies are ok
- A Lie Online is like a job application – your taking out the rough edges
- Confidence issues
- It's better to be forgiven than to ask for permission
- Happens and is expected on most dating websites, job applications, and others.

Your looking at this

What you get is… something better!

Real Penetration Assignment

- Asked to obtain sensitive and confidential information from an organization in an approved penetration tests.
- We were lazy and not very good at programming.
- We thought very least we could have fun and maybe embarrass some people.
- We wanted to avoid Pizza ☺

Warning!

- This talk focuses on **Facebook** & LinkedIN as a method to launch sophisticated attacks **HOWEVER** these are not the only Social Engineering attack vectors!

- *Creating a fake person*
- *Social Engineering on Facebook and LinkedIN*
- *Launch attacks from Social Media sources*
- *Lessons Learned*

Who Are Your Cyber Friends

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Josephine ???

The Facts

- **1 in 5 Couples meet online.**
- **1 in 5 also blame divorce on Facebook**
- **65% of US college students would rather give up sex than the Internet**

- **Facebook passed Google - most visited internet site.**
  - ***11% of world’s population has Facebook account.***
  - ***More Facebook accounts than automobiles.***
  - ***If Facebook were a country, it would be the 3rd largest in the world***

Robin Sage

- **Fictional** American cyber threa created to abstract sensiti on. She graduated from M 10 years of experien she was **25** years old.

What Is The Real Threat?

- ake profile, she was offered ing work with notable companies ch as Google and Lockheed Marti. She had friends in the FBI, CIA and even offered dinner invitations from male friends.

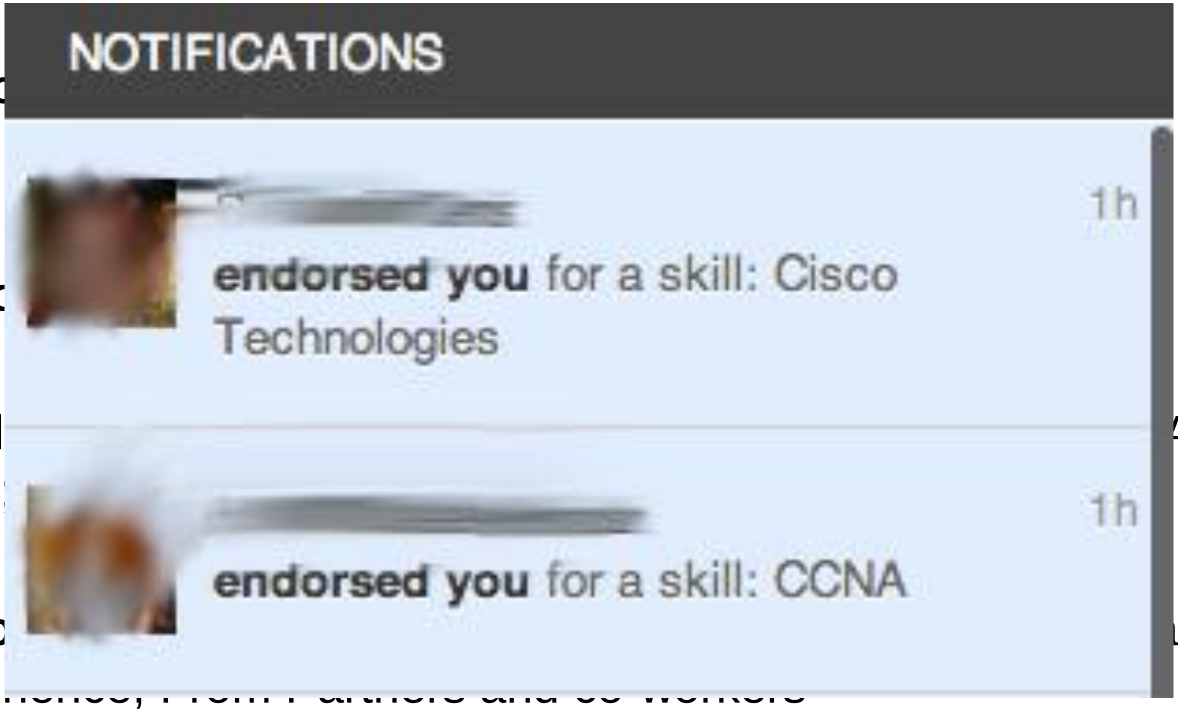
Meet Emily Williams

- Fictional CSE created to abstract sensitive information from a specific target. She graduated from MIT and had 10 years of experience despite she was 28 years old.

- Despite the fake profile, she was offered sensitive information from our target's AM and CSEs. She had friends in large partner vendors and even offered dinner invitations from male friends.

The Impact of Social Media

- **10 minutes:** **20 Facebook connections**
- **6 LinkedIn Connections**
- **15 ho**
- **24 ho**
- **Total** App; 10 EMC:
- **Endo** nd Experience; From Partners and co-workers
- **Offers:** 4 job offers, Laptop and office equipment, network access.

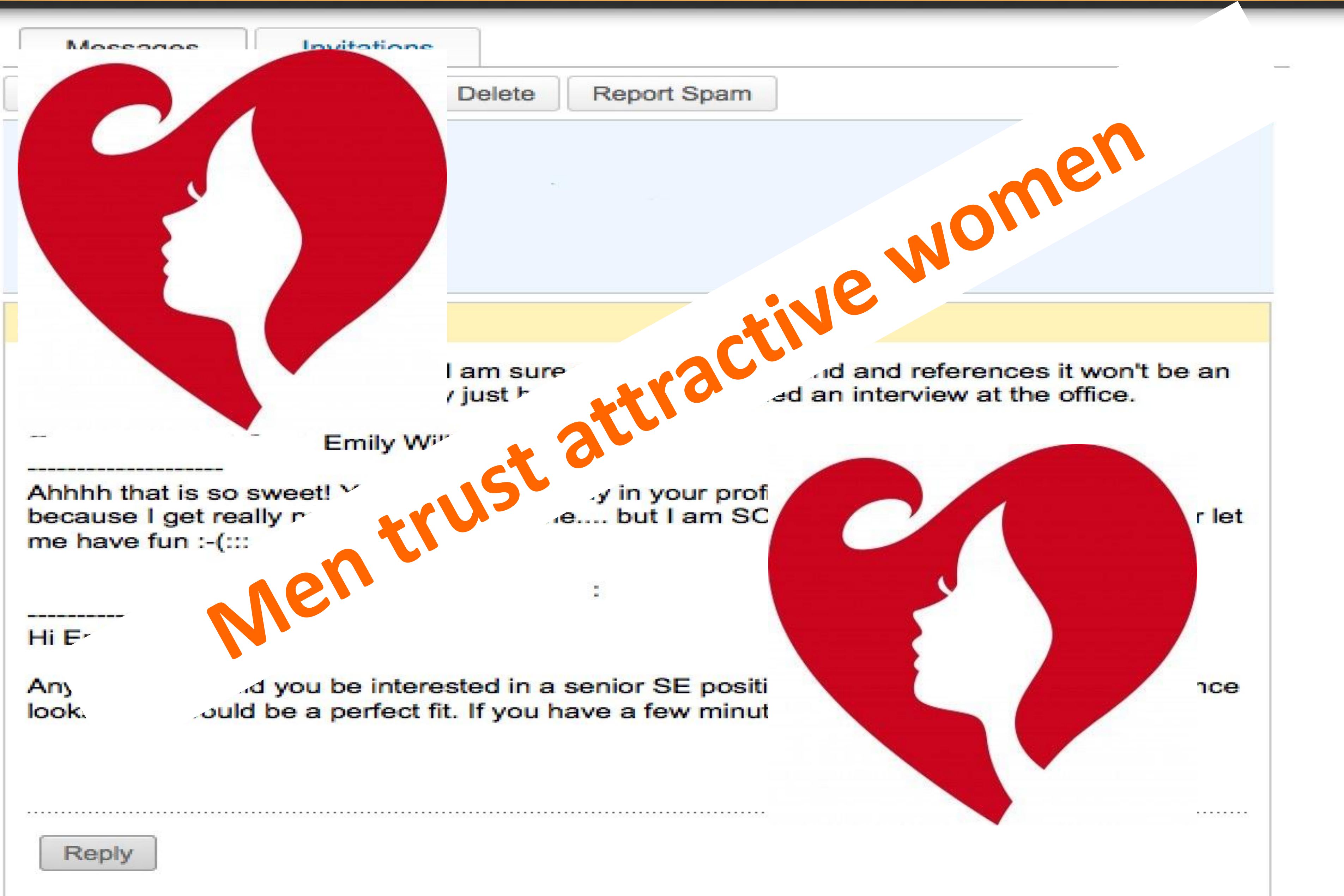


NOTIFICATIONS

[redacted] 1h
endorsed you for a skill: Cisco Technologies

[redacted] 1h
endorsed you for a skill: CCNA

People Trust People



I am sure ... nd and references it won't be an
y just h ... ed an interview at the office.

Emily Wi

Ahhhh that is so sweet! Y ... y in your profi
because I get really n ... e.... but I am SO ... r let
me have fun :-(:::

:

Hi E

Any ... d you be interested in a senior SE positi ... nce
look ... ould be a perfect fit. If you have a few minut

Men trust attractive women

What did we do?

- ***What?***

- **Created fake FaceBook and LinkedIn profile to gain information using social media.**

- ***How?***

- **Social engineering techniques that allowed us to participate as a New Hire**

- ***What was captured?***

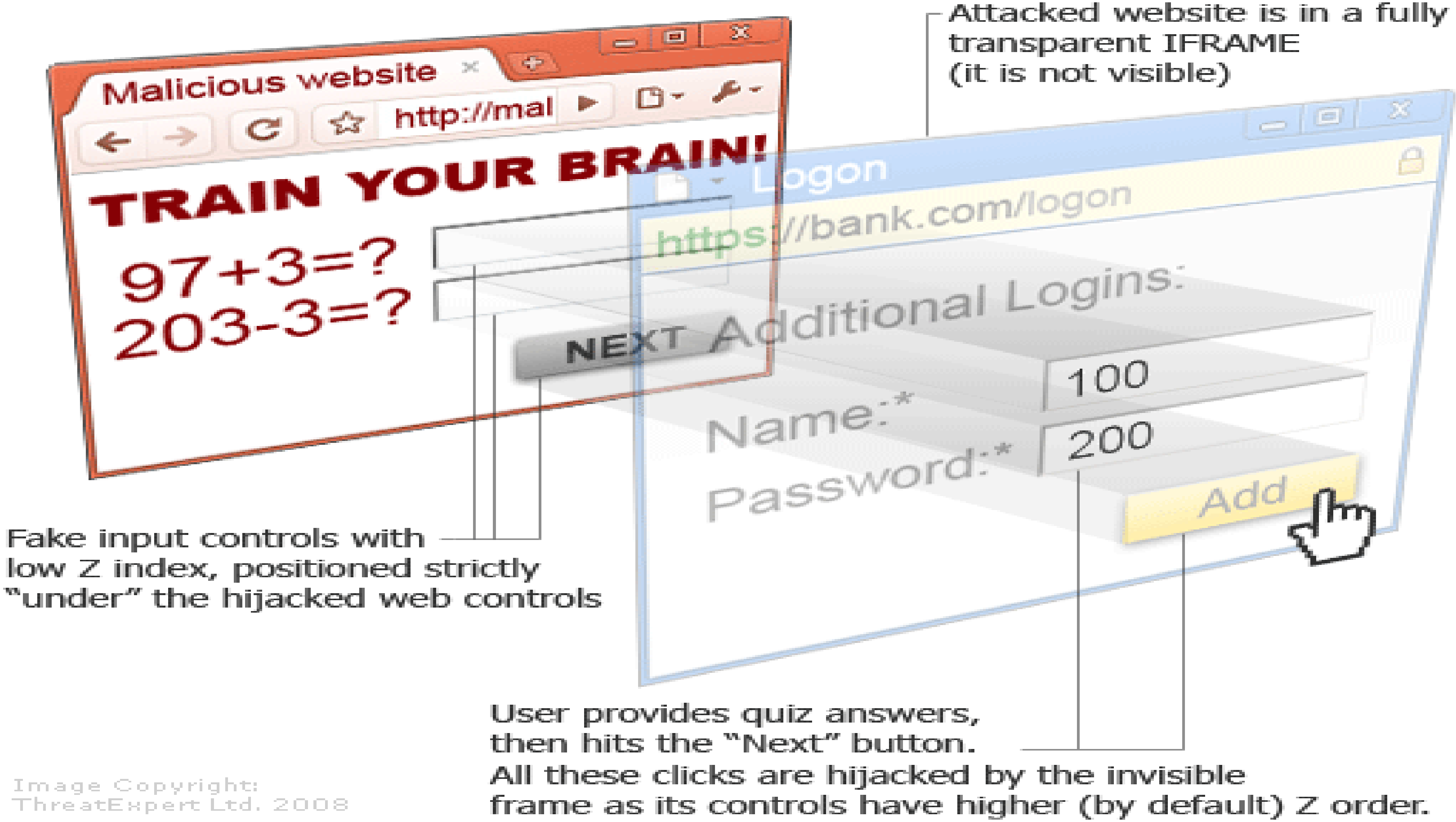
- **Salesforce Logins, Issued Laptops, Jobs offers, Endorsements, Meet up requests**

- ***What was the real threat?***

- **Published a Christmas card on social networks that gave us remote access to anyone that clicked on the link. This gave us significant access to devices and data.**

Happy Holidays

Click Jacking



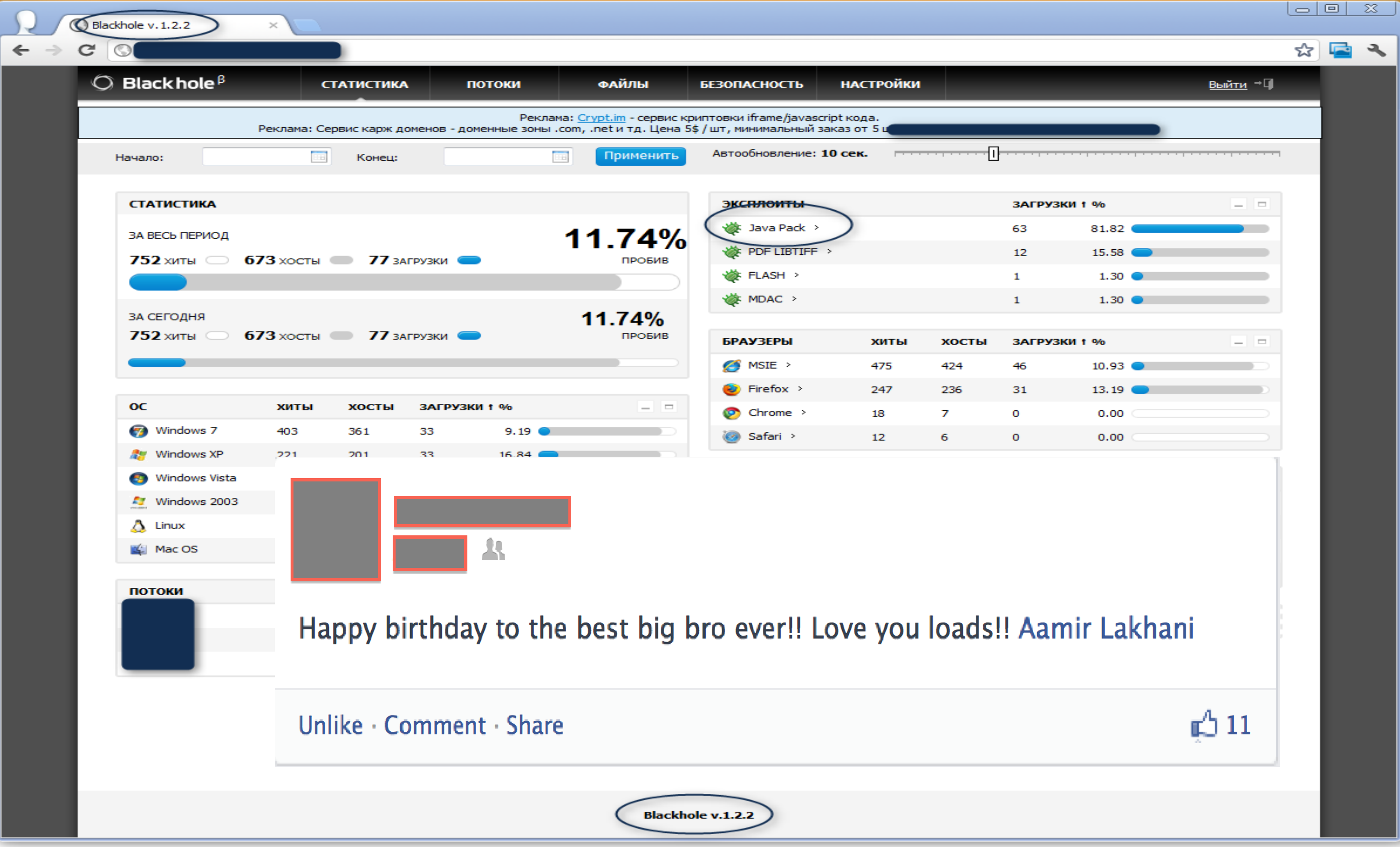
Attacked website is in a fully transparent IFRAME (it is not visible)

Fake input controls with low Z index, positioned strictly "under" the hijacked web controls

User provides quiz answers, then hits the "Next" button. All these clicks are hijacked by the invisible frame as its controls have higher (by default) Z order.

Image Copyright: ThreatExpert Ltd. 2008

Malware



Blackhole v.1.2.2

[redacted]

Реклама: Crypt.im - сервис криптовки iframe/javascript кода.
Реклама: Сервис карж доменов - доменные зоны .com, .net и тд. Цена 5$ / шт, минимальный заказ от 5 [redacted]

Начало: Конец: Применить Автообновление: **10 сек.**

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

752 ХИТЫ **673** ХОСТЫ **77** ЗАГРУЗКИ

11.74% ПРОБИВ

ЗА СЕГОДНЯ

752 ХИТЫ **673** ХОСТЫ **77** ЗАГРУЗКИ

11.74% ПРОБИВ

ЭКСПЛОИТЫ	ЗАГРУЗКИ ↑	%
Java Pack ›	63	81.82
PDF LIBTIFF ›	12	15.58
FLASH ›	1	1.30
MDAC ›	1	1.30

БРАУЗЕРЫ	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ ↑	%
MSIE ›	475	424	46	10.93
Firefox ›	247	236	31	13.19
Chrome ›	18	7	0	0.00
Safari ›	12	6	0	0.00

ОС	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ ↑	%
Windows 7	403	361	33	9.19
Windows XP	221	201	33	16.84
Windows Vista				
Windows 2003				
Linux				
Mac OS				

ПОТОКИ

[redacted]

[redacted]

[redacted]

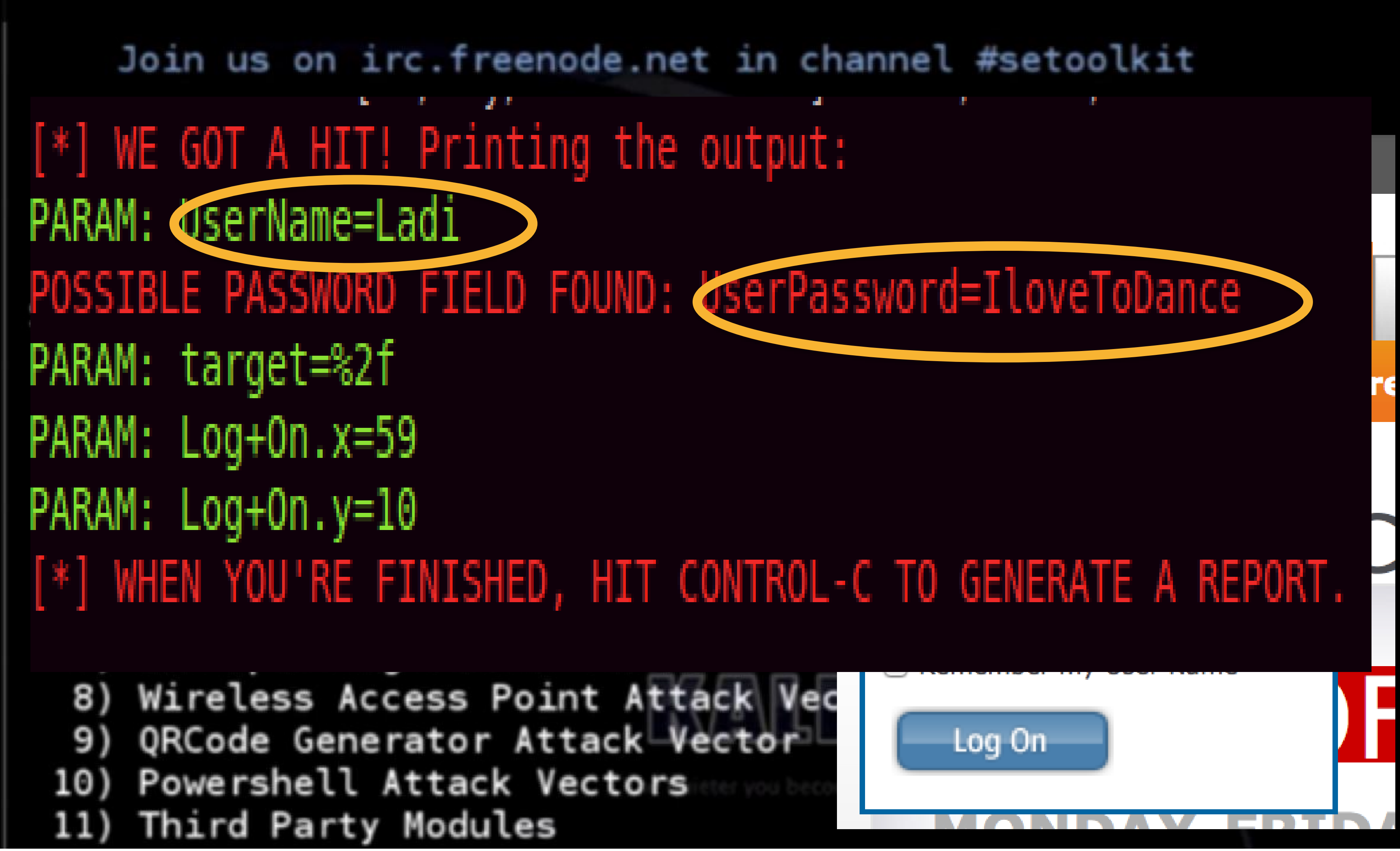
[redacted]

Happy birthday to the best big bro ever!! Love you loads!! Aamir Lakhani

Unlike · Comment · Share 👍 11

Blackhole v.1.2.2

Social Engineering Toolkit

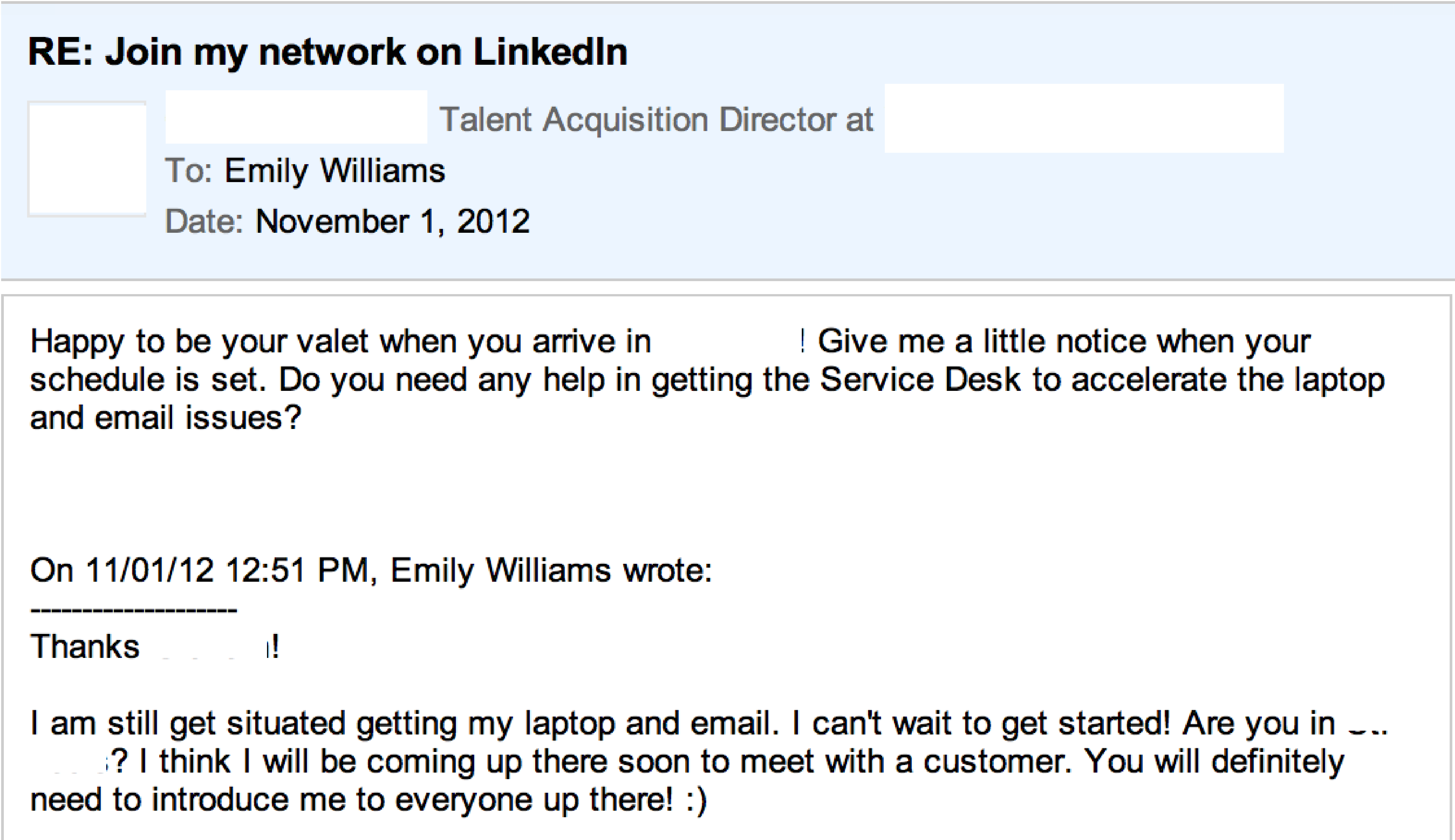


```
    Join us on irc.freenode.net in channel #setoolkit

[*] WE GOT A HIT! Printing the output:
PARAM: UserName=Ladi
POSSIBLE PASSWORD FIELD FOUND: UserPassword=IloveToDance
PARAM: target=%2f
PARAM: Log+On.x=59
PARAM: Log+On.y=10
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

  8) Wireless Access Point Attack Vec
  9) QRCode Generator Attack Vector
 10) Powershell Attack Vectors
 11) Third Party Modules
```

What does Emily Teach Us?

- **Identities are a valuable commodity**
- **Humans are naturally trusting**
- **People use the same passwords for everything!**
- **Attractive women get special treatment in a male dominated industry**
- **Common security products will not protect you from Social Engineering**
- **Social Engineering threats can impact your business.**
- **There isn’t a silver bullet product that can protect you from a future Emily Williams**

When is helpful too helpful?



RE: Join my network on LinkedIn

[redacted] Talent Acquisition Director at [redacted]

To: Emily Williams

Date: November 1, 2012

Happy to be your valet when you arrive in [redacted]! Give me a little notice when your schedule is set. Do you need any help in getting the Service Desk to accelerate the laptop and email issues?

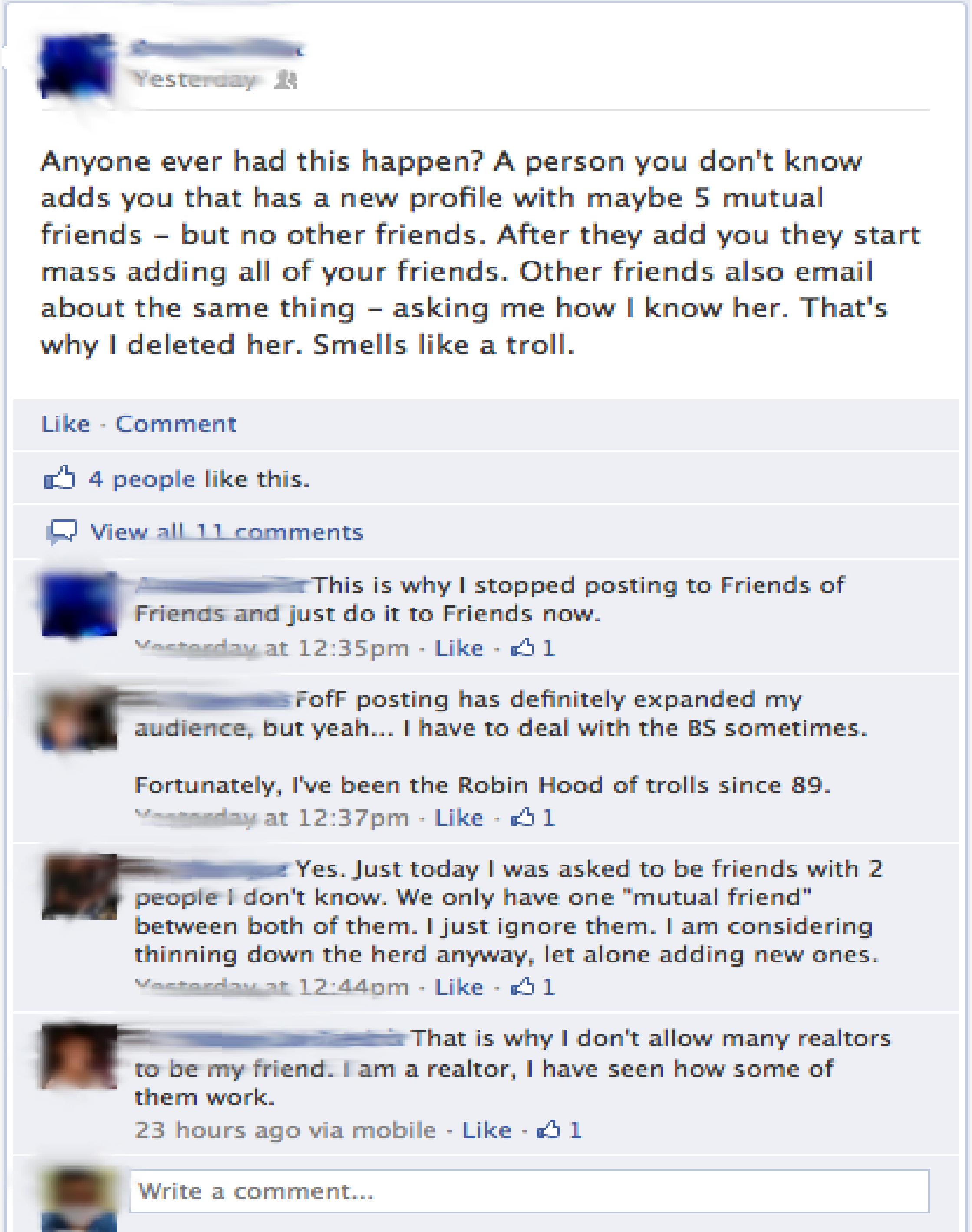
On 11/01/12 12:51 PM, Emily Williams wrote:

Thanks [redacted]!

I am still get situated getting my laptop and email. I can't wait to get started! Are you in [redacted]? I think I will be coming up there soon to meet with a customer. You will definitely need to introduce me to everyone up there! :)

- Some pe

- **Some pe**



[redacted]
Yesterday

Anyone ever had this happen? A person you don't know adds you that has a new profile with maybe 5 mutual friends – but no other friends. After they add you they start mass adding all of your friends. Other friends also email about the same thing – asking me how I know her. That's why I deleted her. Smells like a troll.

[redacted] This is why I stopped posting to Friends of Friends and just do it to Friends now.
Yesterday at 12:35pm · Like · 1

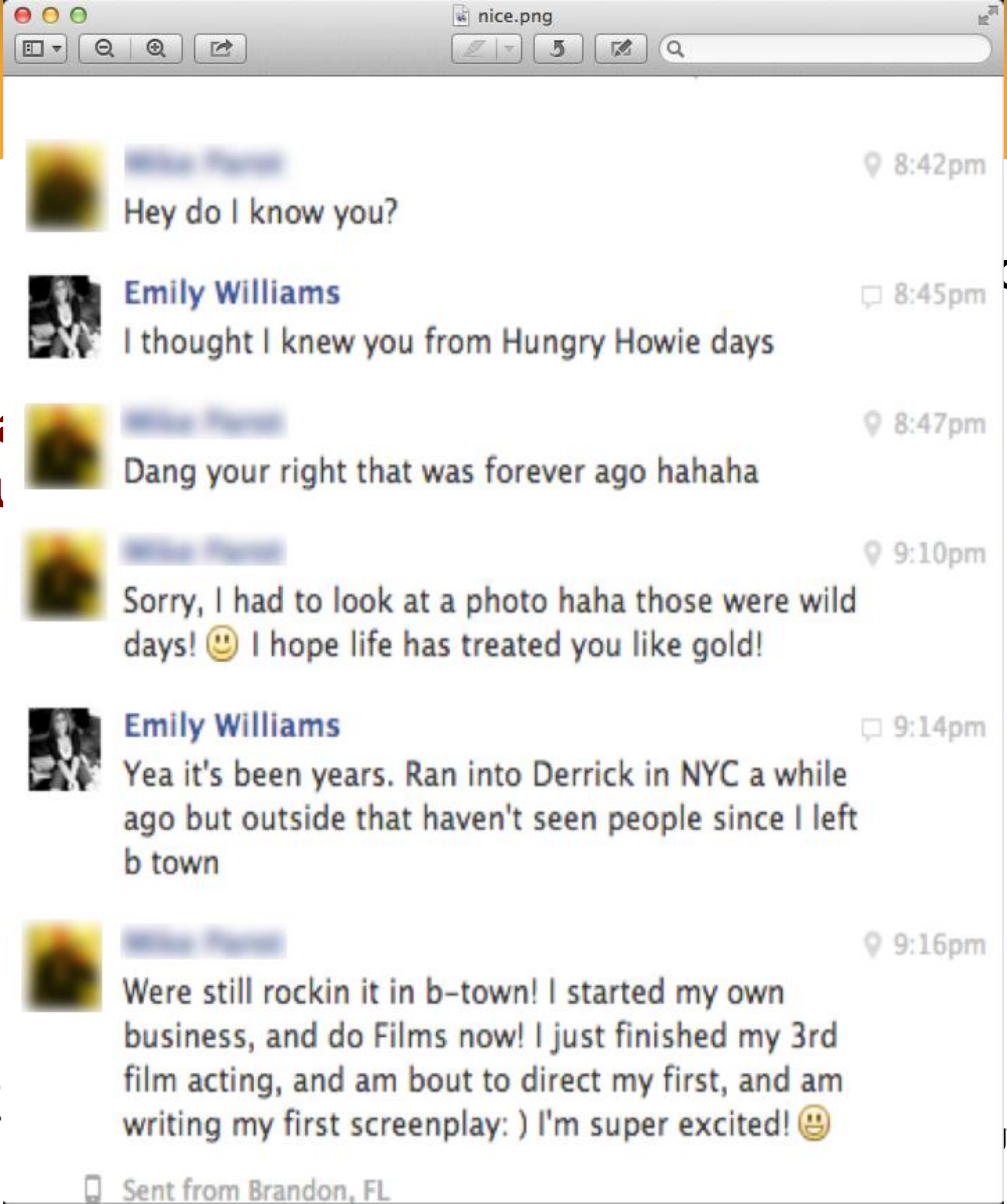
[redacted] FofF posting has definitely expanded my audience, but yeah... I have to deal with the BS sometimes.

Fortunately, I've been the Robin Hood of trolls since 89.
Yesterday at 12:37pm · Like · 1

[redacted] Yes. Just today I was asked to be friends with 2 people I don't know. We only have one "mutual friend" between both of them. I just ignore them. I am considering thinning down the herd anyway, let alone adding new ones.
Yesterday at 12:44pm · Like · 1

[redacted] That is why I don't allow many realtors to be my friend. I am a realtor, I have seen how some of them work.
23 hours ago via mobile · Like · 1

- We ou!
- **Wha could be u**



[redacted] 8:42pm
Hey do I know you?

Emily Williams 8:45pm
I thought I knew you from Hungry Howie days

[redacted] 8:47pm
Dang your right that was forever ago hahaha

[redacted] 9:10pm
Sorry, I had to look at a photo haha those were wild days! 🙂 I hope life has treated you like gold!

Emily Williams 9:14pm
Yea it's been years. Ran into Derrick in NYC a while ago but outside that haven't seen people since I left b town

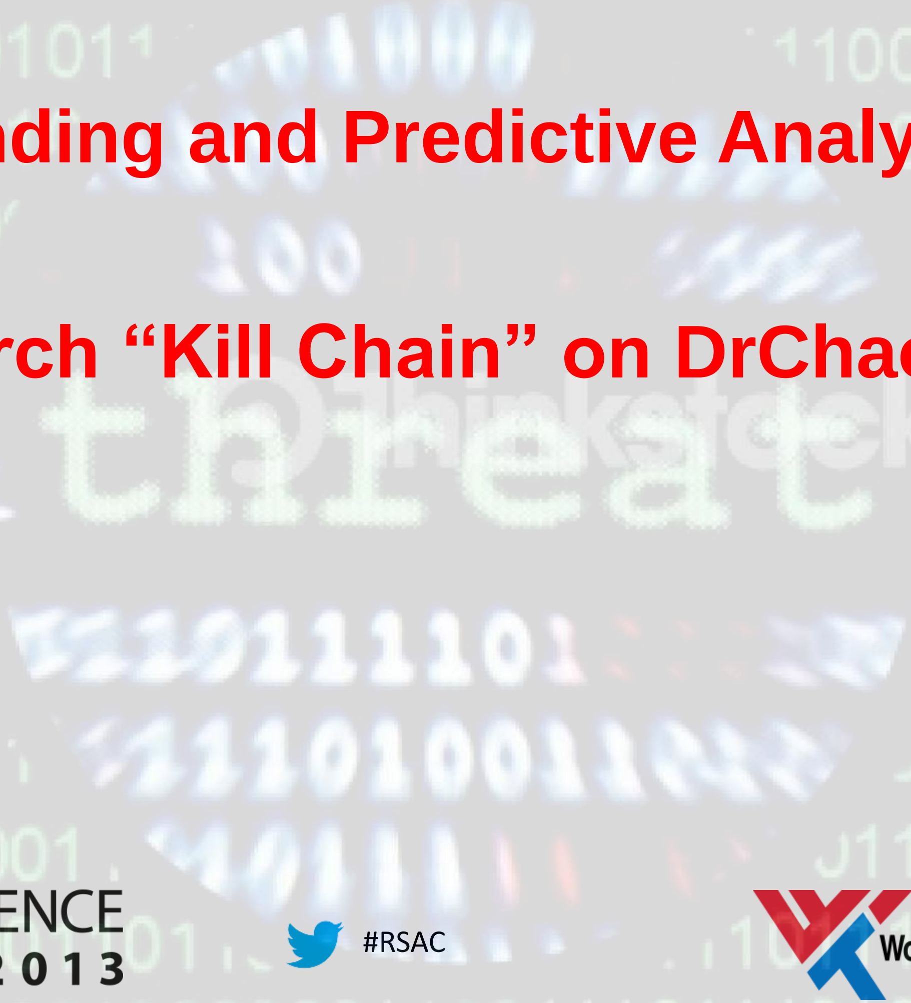
[redacted] 9:16pm
Were still rockin it in b-town! I started my own business, and do Films now! I just finished my 3rd film acting, and am bout to direct my first, and am writing my first screenplay:) I'm super excited! 😃

Sent from Brandon, FL

Social Engineering Best Practices

- ***Segment the network***
- ***Provide limited approved access***
- ***Spread your security investments***
- ***Next generation XYZ isn’t a silver bullet***
- ***Attack your own network***
- ***Use your data or its worthless***

Big Data Security Analytics



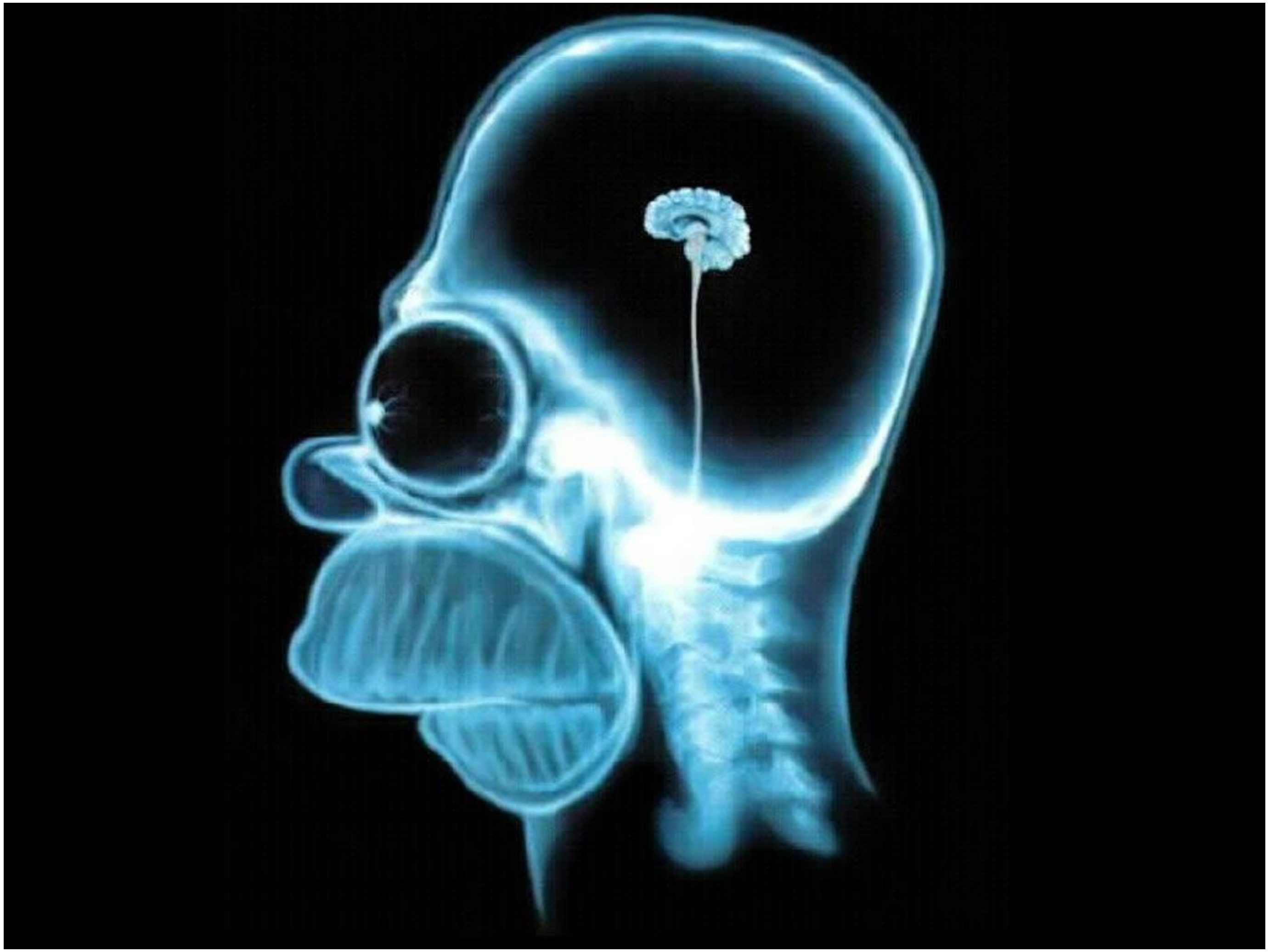
- ► **Hot, Warm, and Cold Data Threats**
- ► **Trending and Predictive Analysis**
- ► **Search “Kill Chain” on DrChaos.com**

Social I asures

- *Questi*
- *Forwa*
- *Be aw*
- *Never*
- *Protec s.*
- *Don't s*

"On the Internet, nobody knows you're a dog."

Can’t Solve Every Problem



Security in knowledge

Thank you!

Aamir Lakhani

World Wide Technology
@aamirlakhani
www.DrChaos.com

www.wwt.com

Joseph Muniz

Cisco Systems

TheSecurityBlogger.com

www.cisco.com