UNIVERSITY OF TEXAS ARLINGTON

Protecting Public Works Infrastructure: Cyber Risk

Rick McCreary

Ashley Mathews

Technology Advances and Expansion

Growing Dependence

- Technological advances create greater dependence
  - Mobile banking
  - Electronic payments

PHOTO: JUSTIN SULLIVAN/GETTY IMAGES

$210 Million

Cyber Risk & Infrastructure

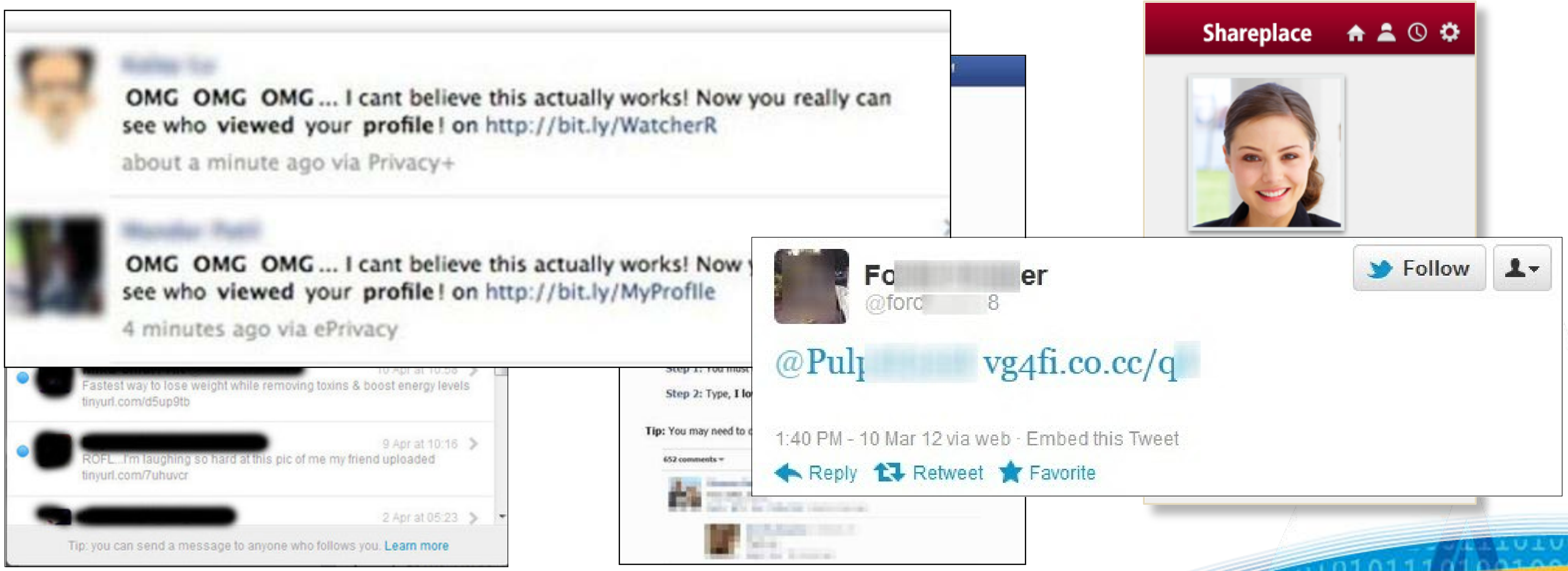
- “Black Hat Researchers Remotely Hack Into SCADA Systems on Oil Rigs”
  - *Demonstrated ability to send commands and fake data, which could cause pipe to burst and a tank to overflow*

Multiple Attacks in 2013

- DHS has set up the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- 200 cyber attacks October 2012 - May 2013
- 53% targeted the energy sector
- Manufacturing was second with 17%
- These were the ones that were reported to DHS!

Evolving Threat Landscape

- Sophisticated means and methods
- Global threat
- Benefit from technology advancement



OMG OMG OMG ... I cant believe this actually works! Now you really can see who viewed your profile! on http://bit.ly/WatcherR

about a minute ago via Privacy+

OMG OMG OMG ... I cant believe this actually works! Now y
see who viewed your profile! on http://bit.ly/MyProfile

4 minutes ago via ePrivacy

[redacted] 10 Apr at 10:58
Fastest way to lose weight while removing toxins & boost energy levels
tinyurl.com/d5up9tb

[redacted] 9 Apr at 10:16
ROFL...I'm laughing so hard at this pic of me my friend uploaded
tinyurl.com/7uhuvcr

[redacted] 2 Apr at 05:23

Tip: you can send a message to anyone who follows you. Learn more

Step 1: You must

Step 2: Type, I lo

Tip: You may need to c

652 comments

Fo er
@forc 8

@Pul vg4fi.co.cc/q

1:40 PM - 10 Mar 12 via web · Embed this Tweet

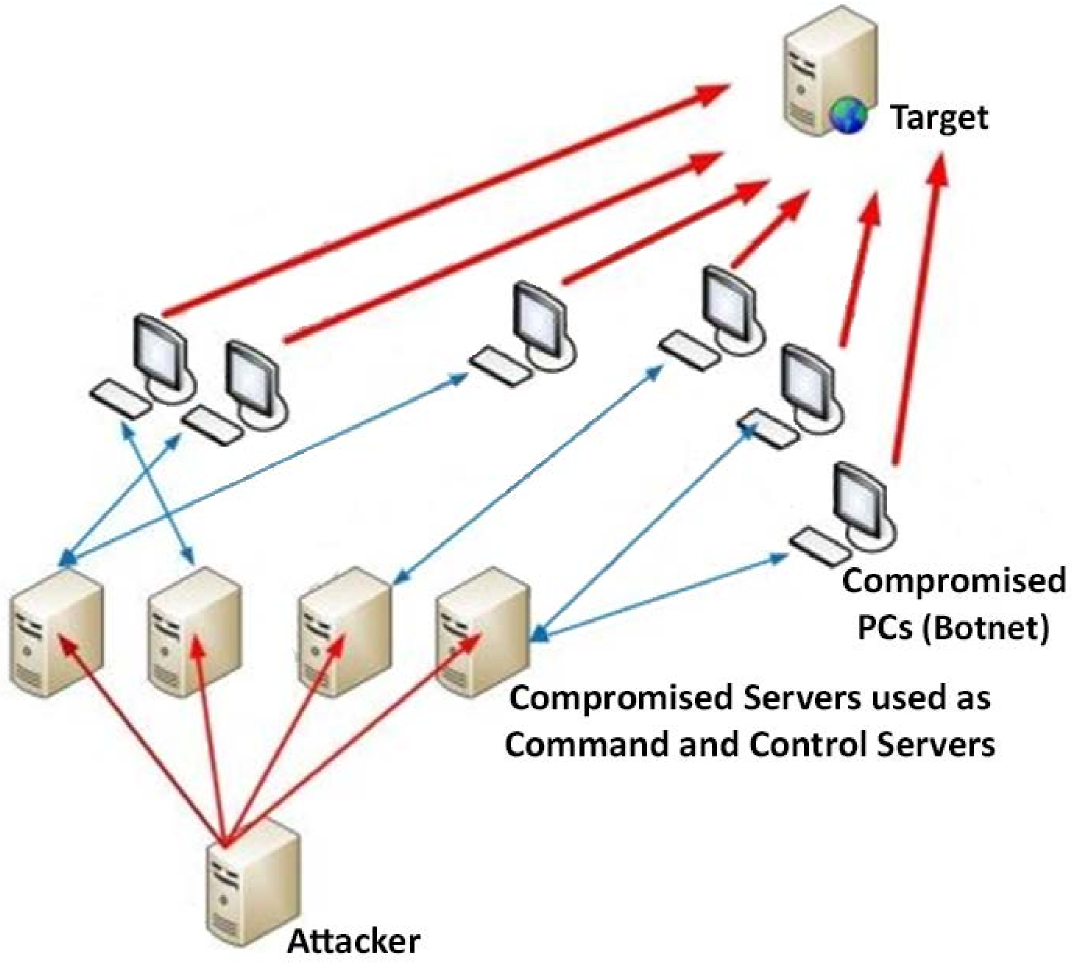
Cyber Risk

Critical Infrastructure

Some Common Cyber Attacks

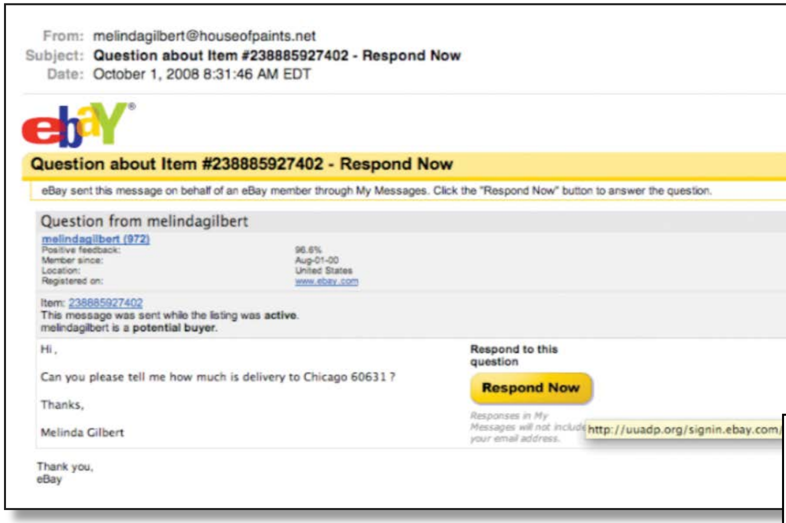
- Distributed Denial of Service (DDoS)
- Phishing and Spear Phishing
- Web Application Attacks
- Advanced Persistent Threats

Distributed Denial of Service (DDoS)



DDOS Attacks on Financial Institutions

Phishing



From: melindagilbert@houseofpaints.net
Subject: **Question about Item #238885927402 - Respond Now**
Date: October 1, 2008 8:31:46 AM EDT

Question about Item #238885927402 - Respond Now

eBay sent this message on behalf of an eBay member through My Messages. Click the "Respond Now" button to answer the question.

Question from melindagilbert

melindagilbert (972)

Positive feedback:	96.6%
Member since:	Aug-01-00
Location:	United States
Registered on:	www.ebay.com

Item: 238885927402
This message was sent while the listing was **active**.
melindagilbert is a **potential buyer**.

Hi ,

Can you please tell me how much is delivery to Chicago 60631 ?

Thanks,

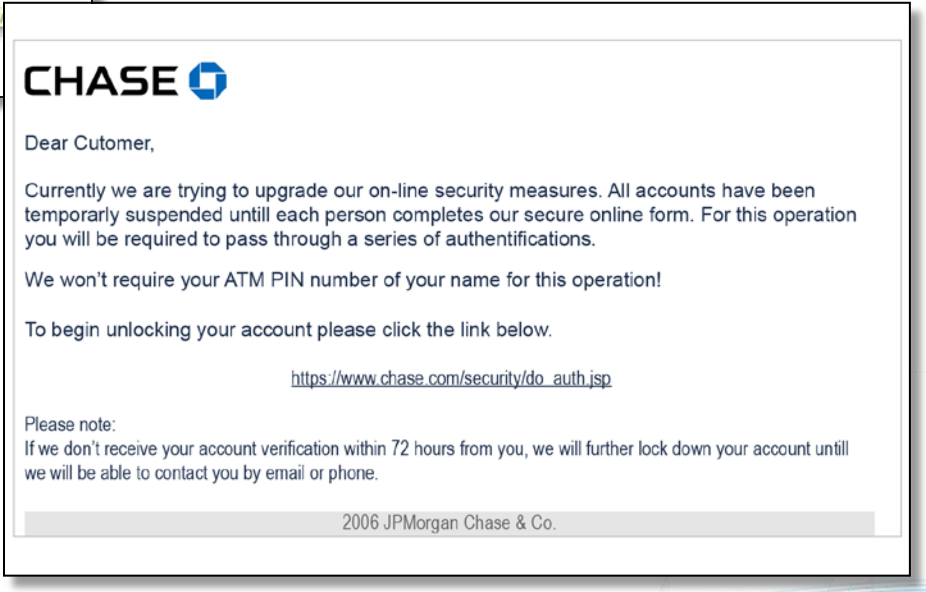
Melinda Gilbert

Respond to this question

Responses in My Messages will not include your email address.

Thank you,
eBay

Phishing generally relies on nonspecific coercive "carrot-and-stick" language to compel users into falling for attackers' schemes.



CHASE

Dear Cutomer,

Currently we are trying to upgrade our on-line security measures. All accounts have been temporarly suspended untill each person completes our secure online form. For this operation you will be required to pass through a series of authentifications.

We won't require your ATM PIN number of your name for this operation!

To begin unlocking your account please click the link below.

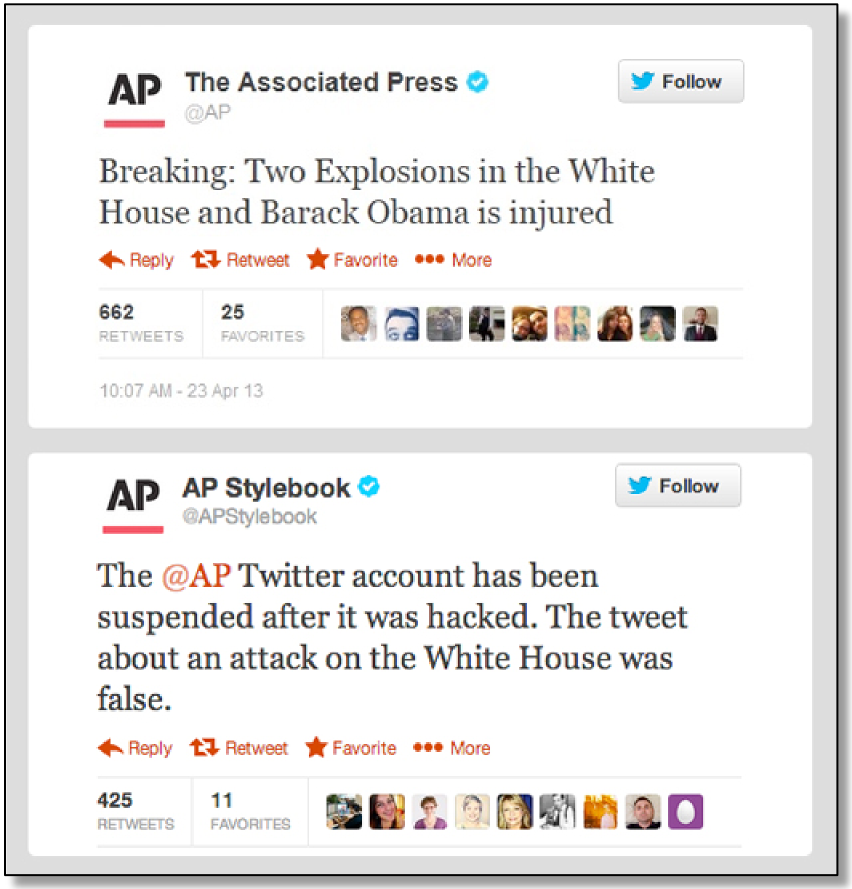
https://www.chase.com/security/do_auth.jsp

Please note:
If we don't receive your account verification within 72 hours from you, we will further lock down your account untill we will be able to contact you by email or phone.

2006 JPMorgan Chase & Co.

Goal is identity theft.

Real World Example - Spear Phishing



AP The Associated Press @AP

Breaking: Two Explosions in the White House and Barack Obama is injured

662 RETWEETS 25 FAVORITES

10:07 AM - 23 Apr 13

AP AP Stylebook @APStylebook

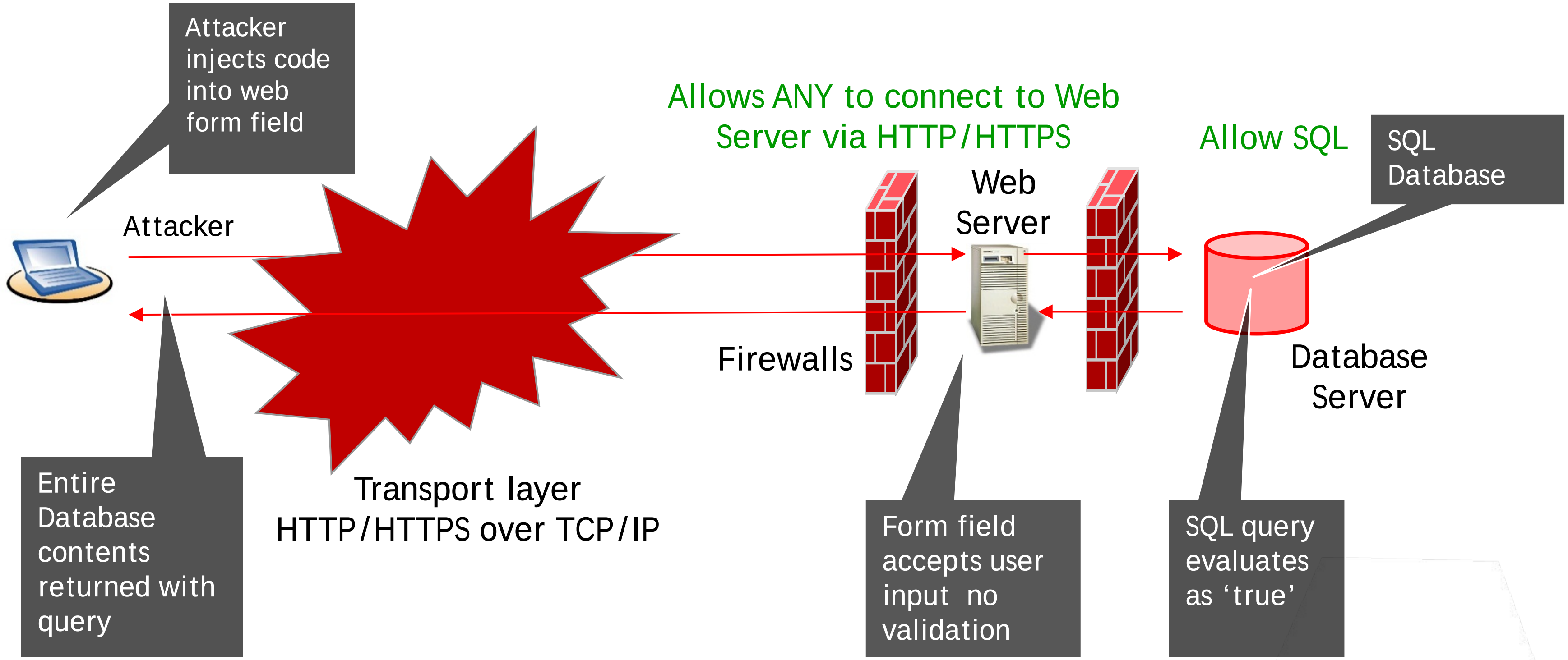
The @AP Twitter account has been suspended after it was hacked. The tweet about an attack on the White House was false.

425 RETWEETS 11 FAVORITES

- Associated Press Twitter Account hacked
- Syrian Electronic Army took credit
- Widespread repercussions

Source: Allison, A. (2013, Apr 23). Hackers compromise ap twitter account, sends stocks plunging. Retrieved from http://www.wset.com/story/22054869/hackers-compromise-ap-twitter-account-sends-stocks-plunging

Web Application Attacks



Attacker injects code into web form field

Allows ANY to connect to Web Server via HTTP/HTTPS

Allow SQL

SQL Database

Entire Database contents returned with query

Form field accepts user input no validation

SQL query evaluates as ‘true’

Advanced Persistent Threat (APT)

- Complex cyber-attacks against specific targets
- Establish and extend access into network
- Remain undetected
- Undermine/impeded critical aspects

“0wN3d”

APT Process

- Once workstation compromised
  - Remotely access network
  - Elevate privileges
  - Gain admin control
  - Compromise other systems through network
  - Retrieve targeted data
  - Erase their tracks

Implications and Consequences

- Financial
- Reputational
- Legal
- Personal

Who are the victims?

37%
Financial Organizations

24%
Retail Environments

20%
Manufacturing, Utilities

20%
IT/Professional Services

38%
Large Corporations

Consequences

Cyber Risk

Questions