# CSE509 : Computer System Security

# Intro / Course Overview

# Why do we want to study Security?

- It is important
- There is never a dull day!
- It is fun!

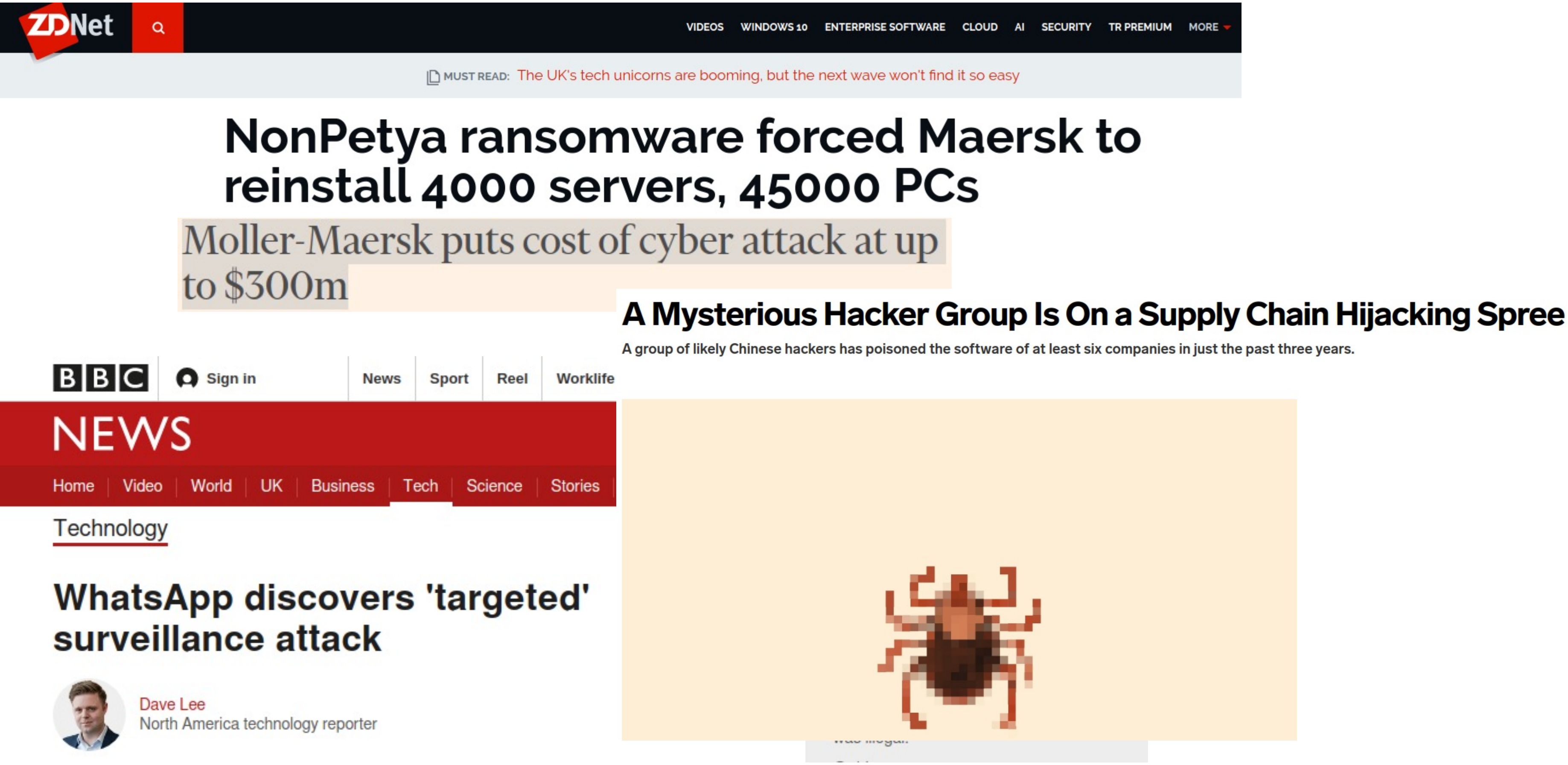
# Security is Important

- An increasing part of our business, social, and personal life involves internet-connected computer systems
  - Web, email, social networks, entertainment, …
  - Mobile computing
  - Cyber-physical systems
  - Internet of things
- Protecting the security and privacy of our digital interactions is critical
  - Most of them involve networked systems and applications

# There is never a dull day!

- Every day, we hear news of yet another high profile hack, data theft, etc.
- New vulnerabilities surface all the time, and we have to find new solutions
- High-stakes game where attackers and defenders innovate constantly in order to stay ahead of each other

# System Security: Never a dull day!



MUST READ: The UK's tech unicorns are booming, but the next wave won't find it so easy

**NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs**

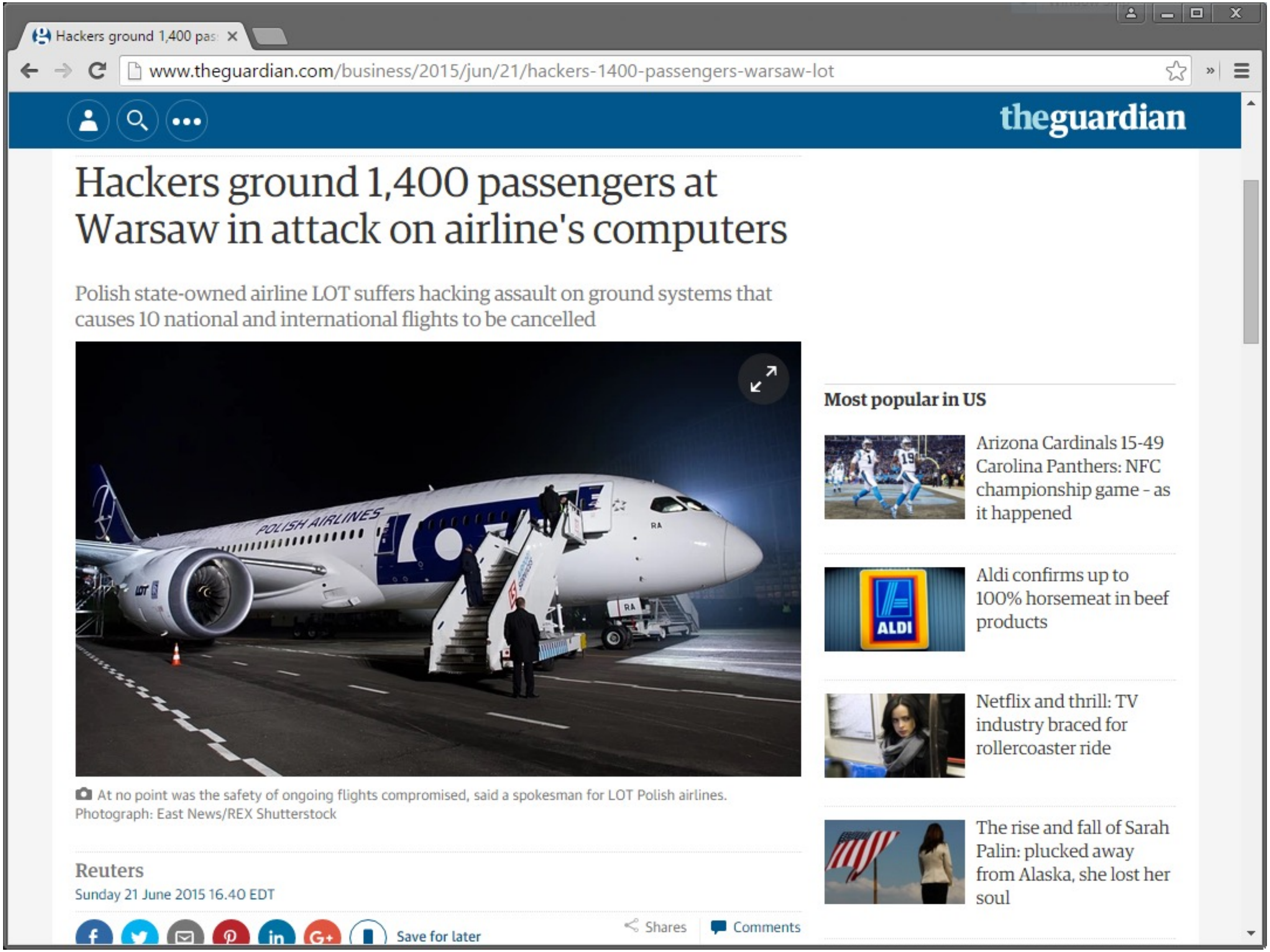
Moller-Maersk puts cost of cyber attack at up to $300m

**A Mysterious Hacker Group Is On a Supply Chain Hijacking Spree**

A group of likely Chinese hackers has poisoned the software of at least six companies in just the past three years.

**WhatsApp discovers 'targeted' surveillance attack**

Dave Lee
North America technology reporter



Hackers ground 1,400 pas ×
www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot
theguardian

# Hackers ground 1,400 passengers at Warsaw in attack on airline's computers

Polish state-owned airline LOT suffers hacking assault on ground systems that causes 10 national and international flights to be cancelled

At no point was the safety of ongoing flights compromised, said a spokesman for LOT Polish airlines. Photograph: East News/REX Shutterstock

Reuters
Sunday 21 June 2015 16.40 EDT

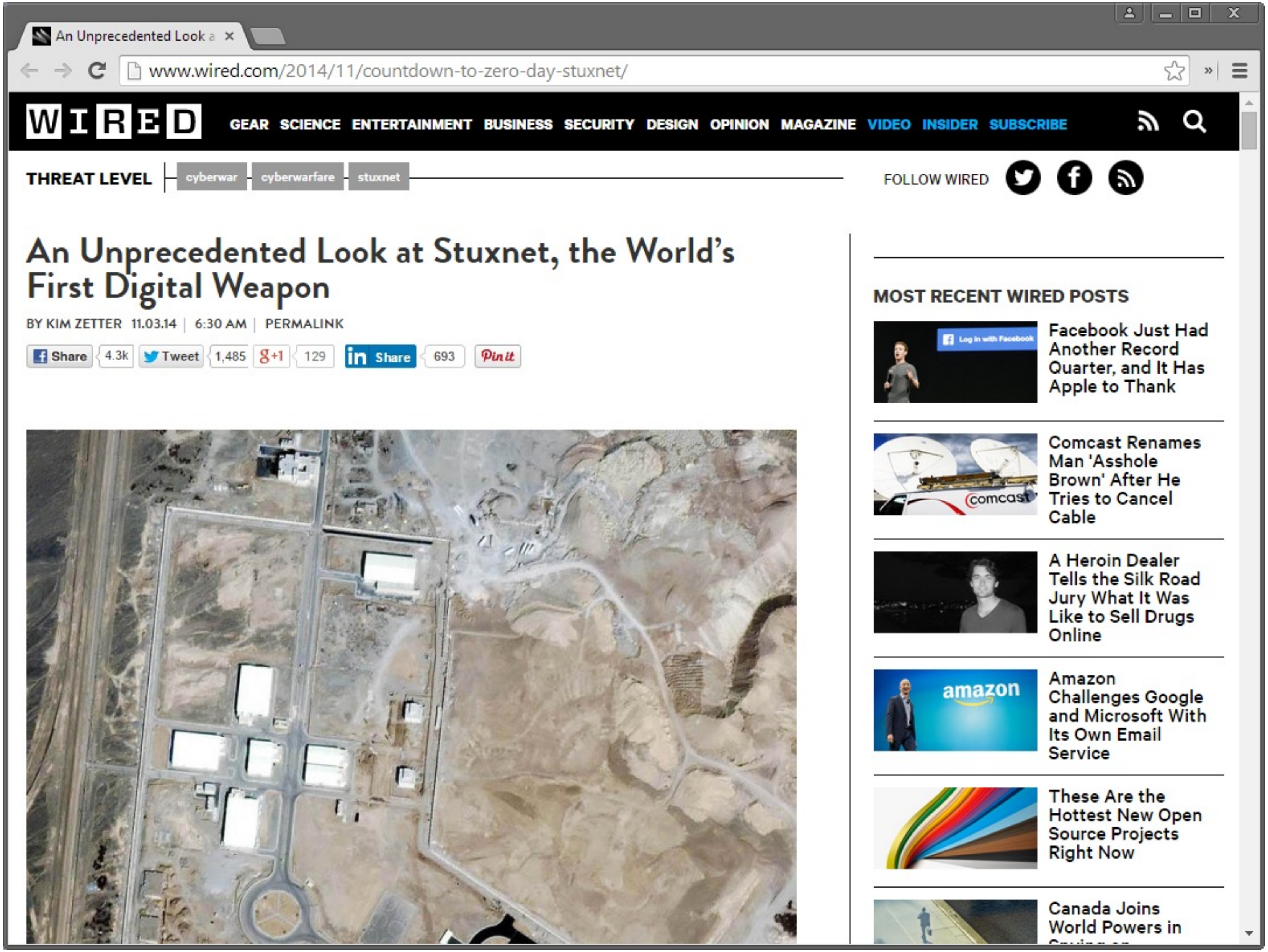
**Most popular in US**

Arizona Cardinals 15-49 Carolina Panthers: NFC championship game - as it happened

Aldi confirms up to 100% horsemeat in beef products

Netflix and thrill: TV industry braced for rollercoaster ride

The rise and fall of Sarah Palin: plucked away from Alaska, she lost her soul



An Unprecedented Look a ×

www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE VIDEO INSIDER SUBSCRIBE

THREAT LEVEL | cyberwar | cyberwarfare | stuxnet

FOLLOW WIRED

# An Unprecedented Look at Stuxnet, the World's First Digital Weapon

BY KIM ZETTER 11.03.14 | 6:30 AM | PERMALINK

Share 4.3k | Tweet 1,485 | g+1 129 | in Share 693 | Pin it

MOST RECENT WIRED POSTS

Facebook Just Had Another Record Quarter, and It Has Apple to Thank

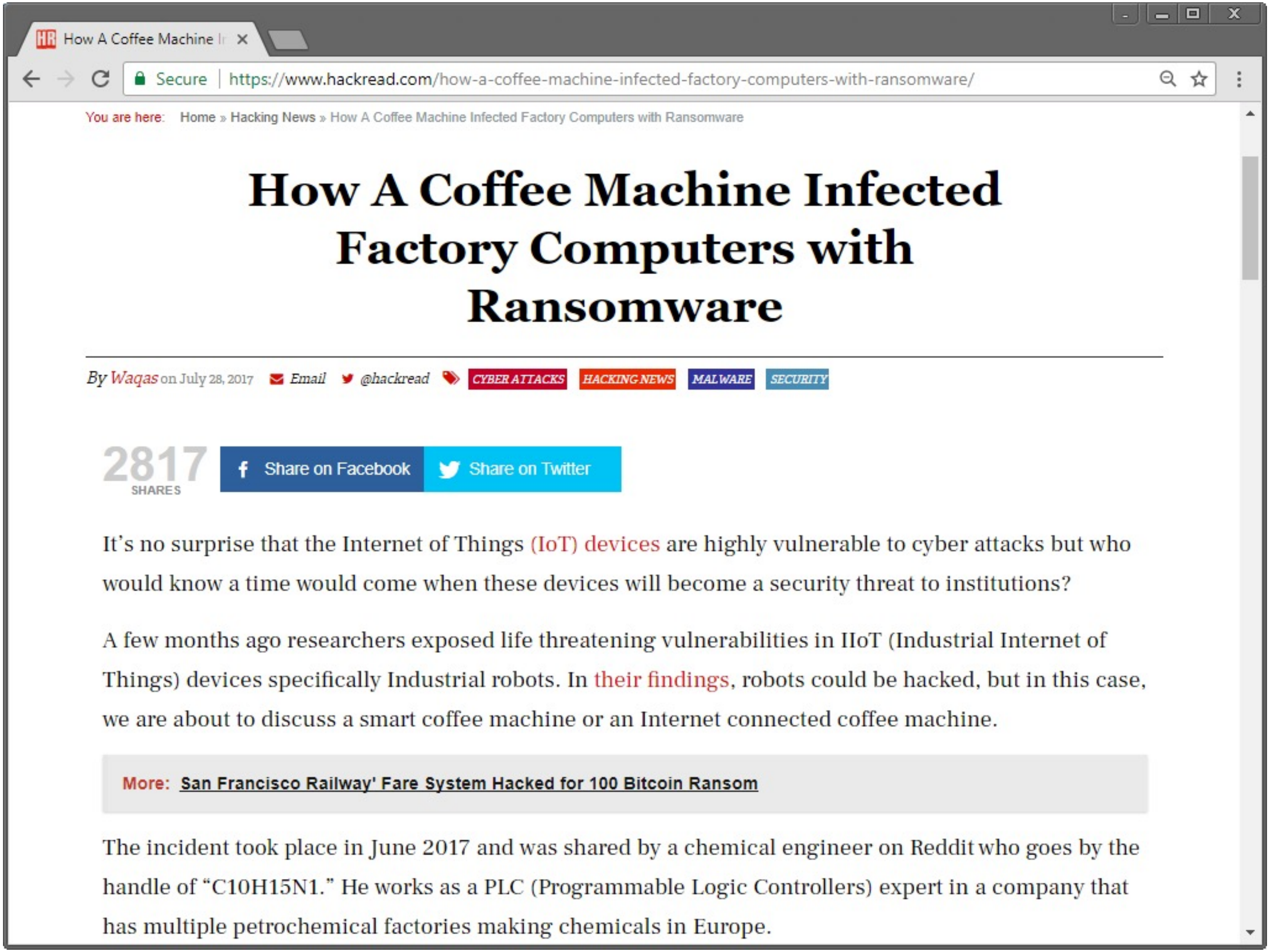
Comcast Renames Man 'Asshole Brown' After He Tries to Cancel Cable

A Heroin Dealer Tells the Silk Road Jury What It Was Like to Sell Drugs Online

Amazon Challenges Google and Microsoft With Its Own Email Service

These Are the Hottest New Open Source Projects Right Now

Canada Joins World Powers in


How A Coffee Machine I
Secure
https://www.hackread.com/how-a-coffee-machine-infected-factory-computers-with-ransomware/

You are here: Home » Hacking News » How A Coffee Machine Infected Factory Computers with Ransomware

# How A Coffee Machine Infected Factory Computers with Ransomware

*By Waqas on July 28, 2017* *Email* *@hackread* *CYBER ATTACKS* *HACKING NEWS* *MALWARE* *SECURITY*

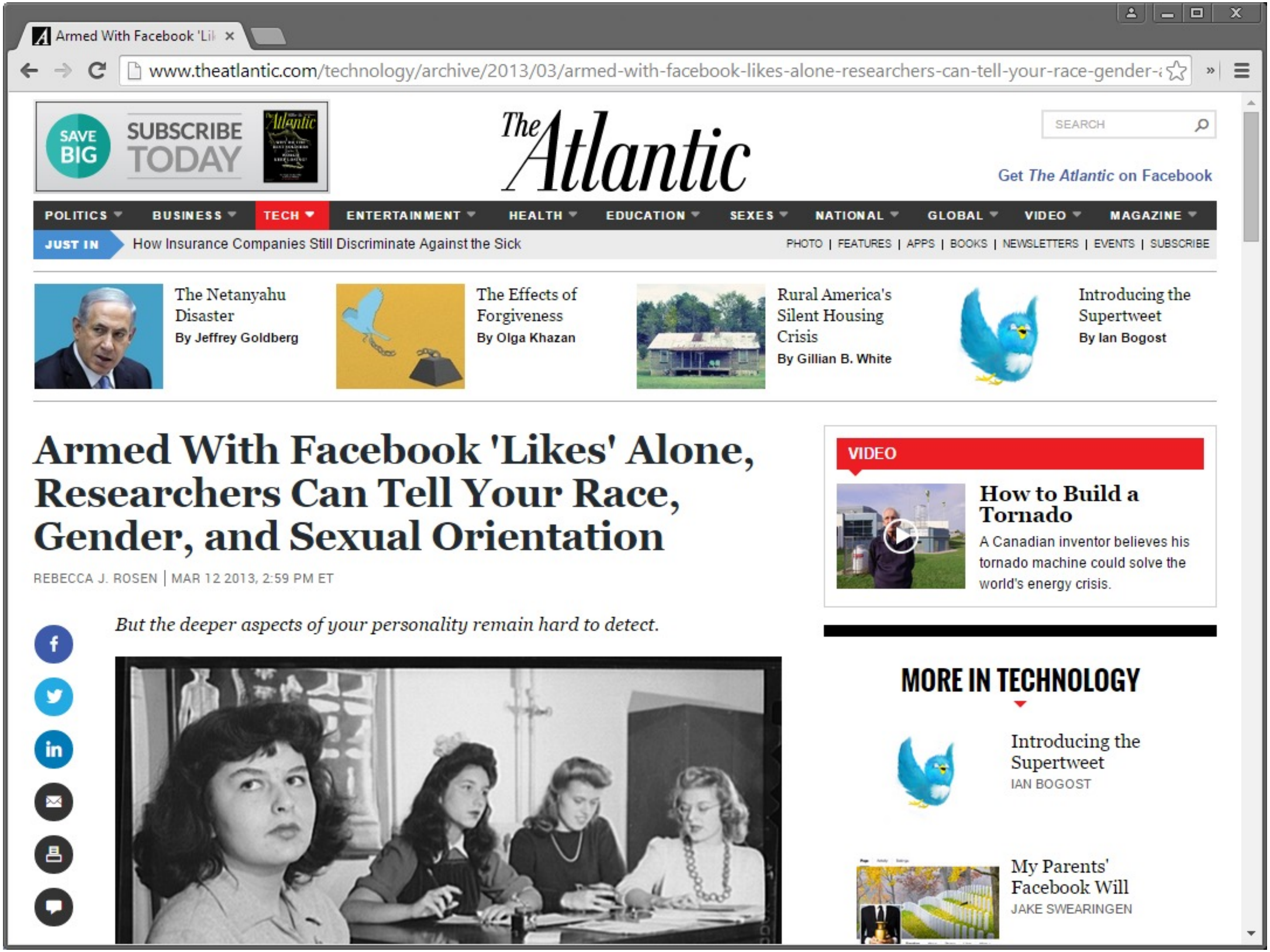
2817
SHARES
Share on Facebook
Share on Twitter

It's no surprise that the Internet of Things (IoT) devices are highly vulnerable to cyber attacks but who would know a time would come when these devices will become a security threat to institutions?

A few months ago researchers exposed life threatening vulnerabilities in IIoT (Industrial Internet of Things) devices specifically Industrial robots. In their findings, robots could be hacked, but in this case, we are about to discuss a smart coffee machine or an Internet connected coffee machine.

**More:** San Francisco Railway' Fare System Hacked for 100 Bitcoin Ransom

The incident took place in June 2017 and was shared by a chemical engineer on Reddit who goes by the handle of "C10H15N1." He works as a PLC (Programmable Logic Controllers) expert in a company that has multiple petrochemical factories making chemicals in Europe.


Armed With Facebook 'Lik
www.theatlantic.com/technology/archive/2013/03/armed-with-facebook-likes-alone-researchers-can-tell-your-race-gender-a
SAVE BIG
SUBSCRIBE TODAY
The Atlantic
SEARCH
Get The Atlantic on Facebook
POLITICS
BUSINESS
TECH
ENTERTAINMENT
HEALTH
EDUCATION
SEXES
NATIONAL
GLOBAL
VIDEO
MAGAZINE
JUST IN
PHOTO | FEATURES | APPS | BOOKS | NEWSLETTERS | EVENTS | SUBSCRIBE

How Insurance Companies Still Discriminate Against the Sick

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

# Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

*But the deeper aspects of your personality remain hard to detect.*

VIDEO

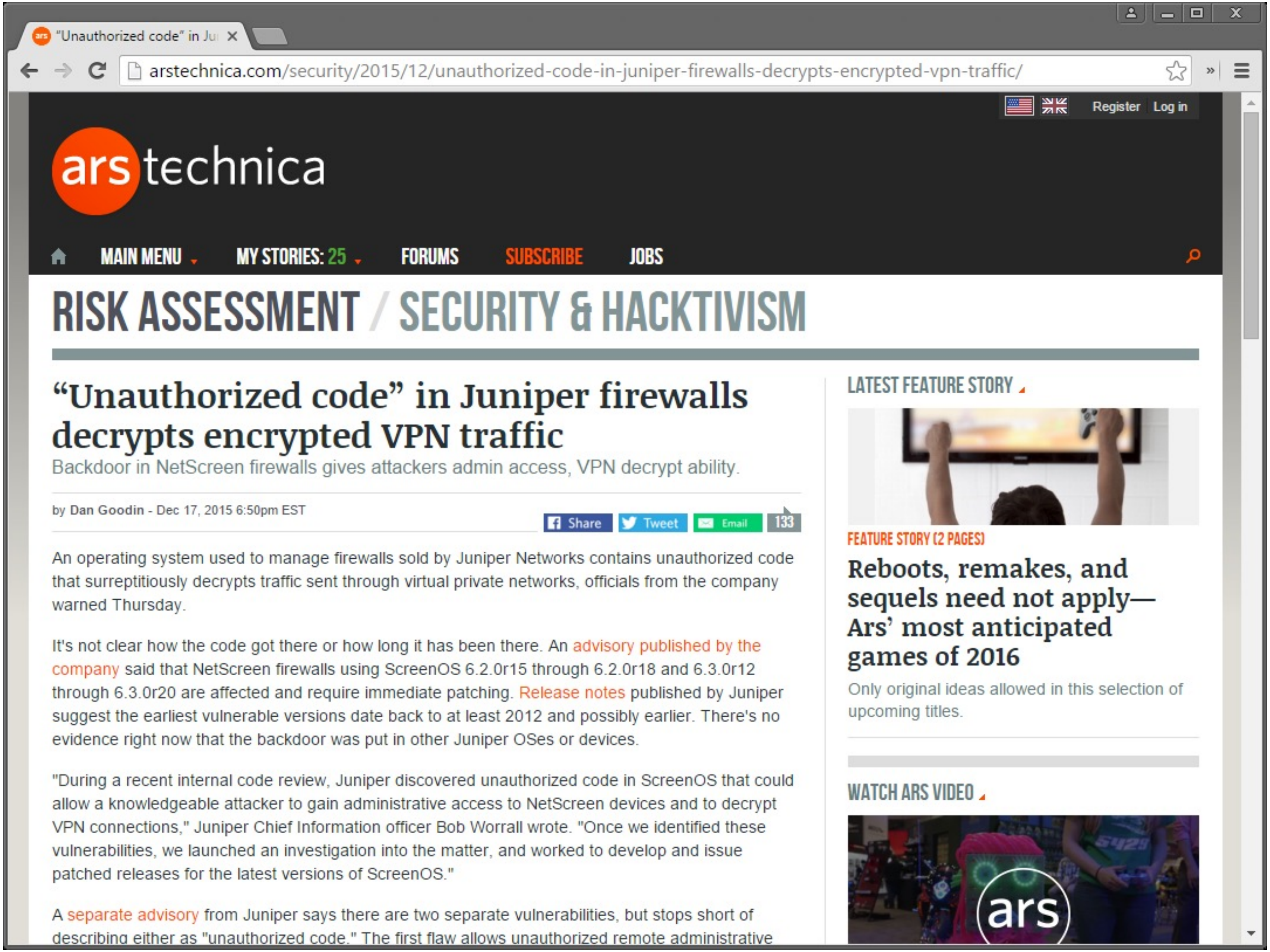
**How to Build a Tornado**

A Canadian inventor believes his tornado machine could solve the world's energy crisis.

MORE IN TECHNOLOGY

Introducing the Supertweet
IAN BOGOST

My Parents' Facebook Will
JAKE SWEARINGEN


"Unauthorized code" in Ju
arstechnica.com/security/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/
Register
Log in
ars technica
MAIN MENU
MY STORIES: 25
FORUMS
SUBSCRIBE
JOBS
Share
Tweet
Email
133
LATEST FEATURE STORY
WATCH ARS VIDEO
ars

RISK ASSESSMENT / SECURITY & HACKTIVISM

# "Unauthorized code" in Juniper firewalls decrypts encrypted VPN traffic

Backdoor in NetScreen firewalls gives attackers admin access, VPN decrypt ability.

by Dan Goodin - Dec 17, 2015 6:50pm EST

An operating system used to manage firewalls sold by Juniper Networks contains unauthorized code that surreptitiously decrypts traffic sent through virtual private networks, officials from the company warned Thursday.

It's not clear how the code got there or how long it has been there. An advisory published by the company said that NetScreen firewalls using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected and require immediate patching. Release notes published by Juniper suggest the earliest vulnerable versions date back to at least 2012 and possibly earlier. There's no evidence right now that the backdoor was put in other Juniper OSes or devices.

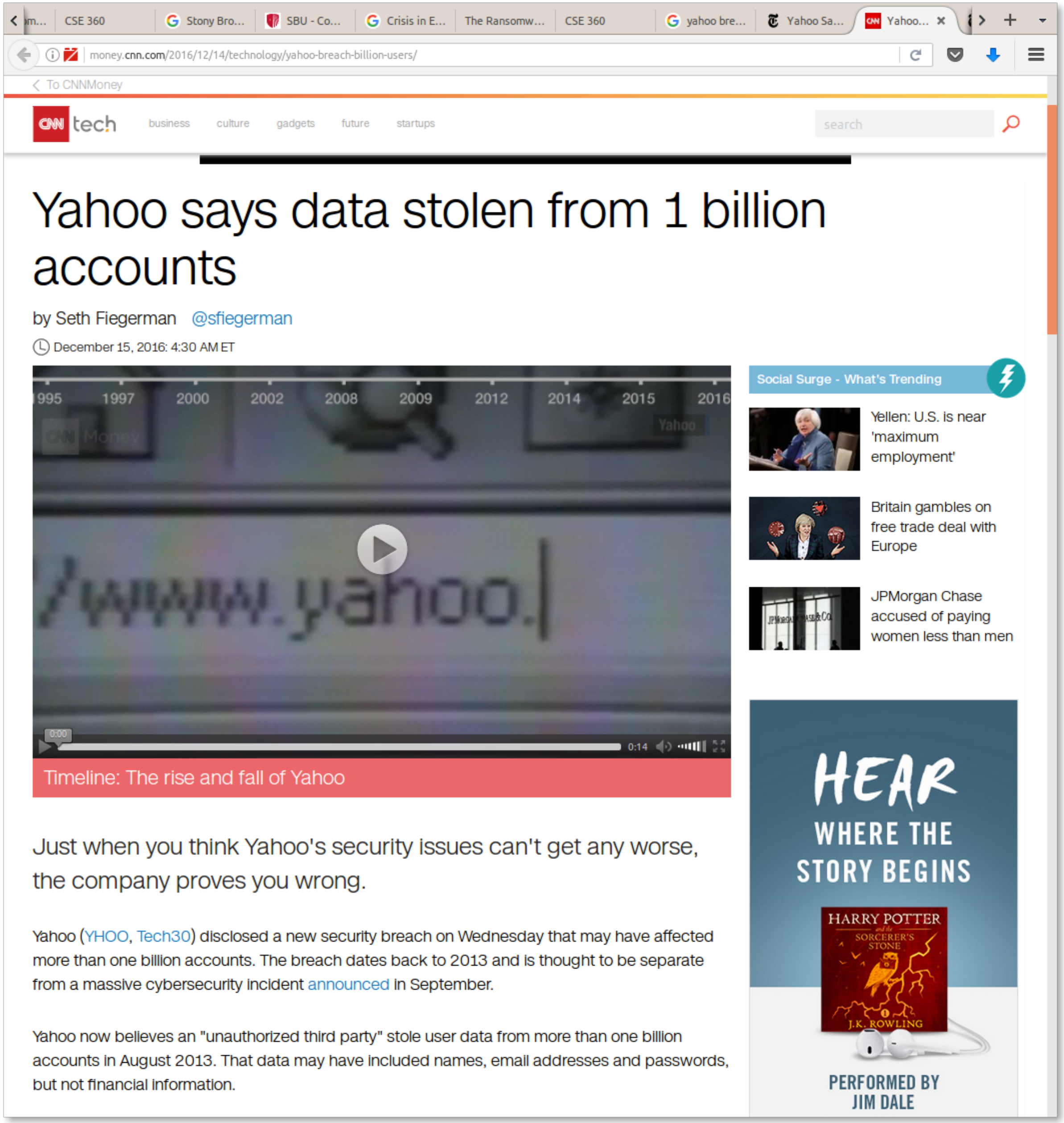
"During a recent internal code review, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices and to decrypt VPN connections," Juniper Chief Information officer Bob Worrall wrote. "Once we identified these vulnerabilities, we launched an investigation into the matter, and worked to develop and issue patched releases for the latest versions of ScreenOS."

A separate advisory from Juniper says there are two separate vulnerabilities, but stops short of describing either as "unauthorized code." The first flaw allows unauthorized remote administrative

FEATURE STORY (2 PAGES)

Reboots, remakes, and sequels need not apply—Ars' most anticipated games of 2016

Only original ideas allowed in this selection of upcoming titles.



# Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

Timeline: The rise and fall of Yahoo

Just when you think Yahoo's security issues can't get any worse, the company proves you wrong.

Yahoo (YHOO, Tech30) disclosed a new security breach on Wednesday that may have affected more than one billion accounts. The breach dates back to 2013 and is thought to be separate from a massive cybersecurity incident announced in September.

Yahoo now believes an "unauthorized third party" stole user data from more than one billion accounts in August 2013. That data may have included names, email addresses and passwords, but not financial information.

Social Surge - What's Trending

Yellen: U.S. is near 'maximum employment'

Britain gambles on free trade deal with Europe

JPMorgan Chase accused of paying women less than men

# System Security: It is fun!

- System security brings together all of the fun CS topics we have learned through other courses
  - Architecture
  - Operating Systems
  - Networks
  - Compilers and Programming Languages
  - Algorithms
  - AI
- System security helps us make connections between these topics, helping us to understand them and remember them better.

# What is security

Wikipedia:

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

# What is computer security?

- Everyone has their own definition
  - No single one is perfect
- Computer security deals with protecting data, programs, and systems against intelligent adversaries.
- Safety vs Security
  - What's the difference between the two?
  - Do they interact?

# CIA

- Security is about CIA
  - *Confidentiality*: Keeping data and resources hidden or protected from unauthorized disclosure
  - *Integrity*: Data and Programs are modified in specified and authorized ways. Data integrity and origin integrity.
  - *Availability*: Systems and networks are available for use by legitimate users

# Why is it hard?

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows have been the "vulnerability of the decade" for multiple decades!
  - Cross-site scripting and other Web attacks
- Networks are more open and accessible than ever
- Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
- Phishing, social engineering, etc.

# Why is it hard?

- It is hard to get security right because:
  - Security is hard to test for
    - Testing correctness versus security
  - It requires a deep understanding of all technologies involved in the design and implementation of a system
    - Really hard in large real systems
  - Users are typically the weakest link
  - *Asymmetry* between attack and defense

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

# Course Focus

- Introduction to a wide range of topics in computer system and software security
  - vulnerabilities, exploit and mitigation techniques
  - malware trends and defenses against untrusted code
  - binary analysis, reverse engineering and forensics
  - software vulnerability scanning techniques and tools
- Cultivate the "security mindset"
  - Understand the modus operandi of attackers: find vulnerabilities, subvert protections, bypass defenses,…
- Hands-on assignments in exploit development and mitigation

# Ethics and Legal Considerations

- Play Fair
- Cannot teach defense without offense, but:

  *Breaking into systems is illegal!*
  *Unauthorized data access is illegal!*

- Computer Fraud and Abuse Act (CFAA)
  - http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf
- Practice on your own systems or controlled environment
- Scanning/penetration testing/etc. of third-party systems may be allowed only after getting permission by their owner

# Code of Conduct

- The work that you present as your own should be your own
- Cite the resources that you used (other people's code, documents, etc.)
- Don't allow your code/paper summaries to be copied
- Don't copy other people's code or paper summaries
- Anything short of the above, will be grounds for immediate "F" grade and further disciplinary action

# Credits

- Some slide contents in this lecture and future ones are courtesy of R. Sekar, Nick Nikiforakis and Michalis Polychronakis

# Questions