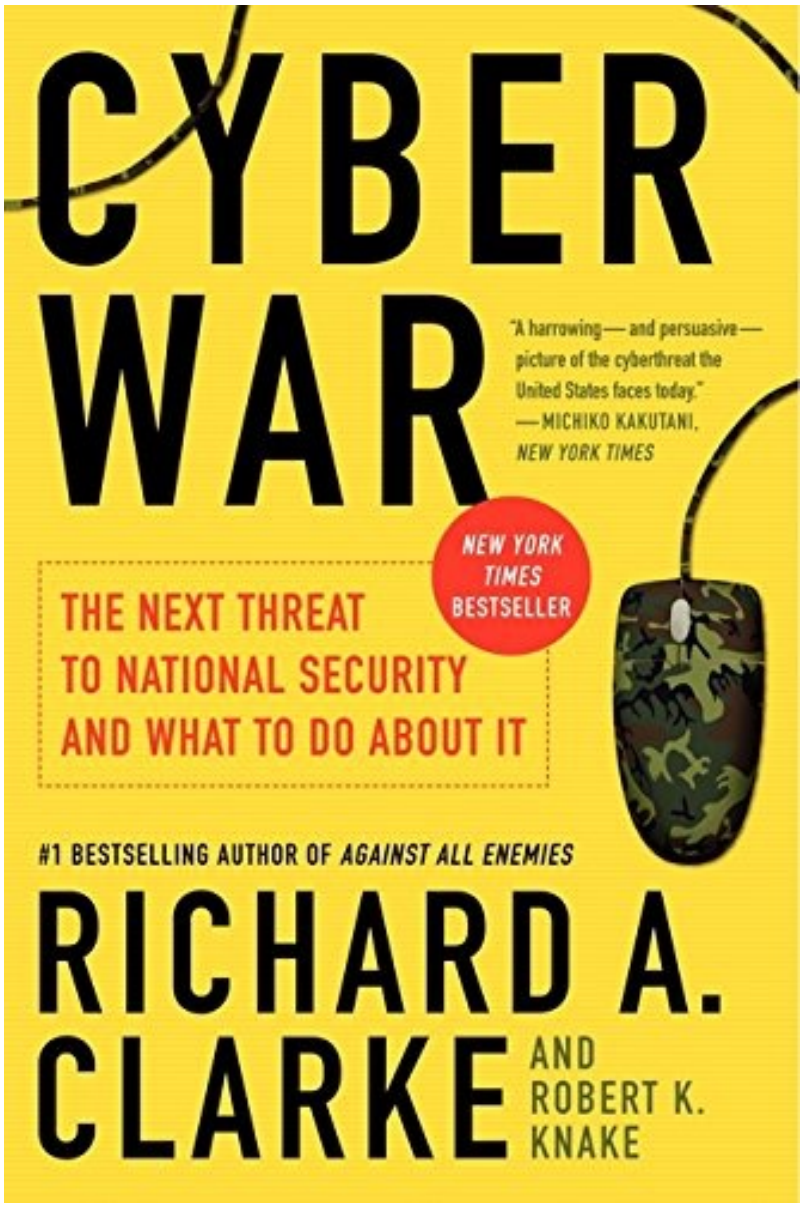
Cyber War and APTs

What is the world coming to??



Slides by Prof. Kevin Fu

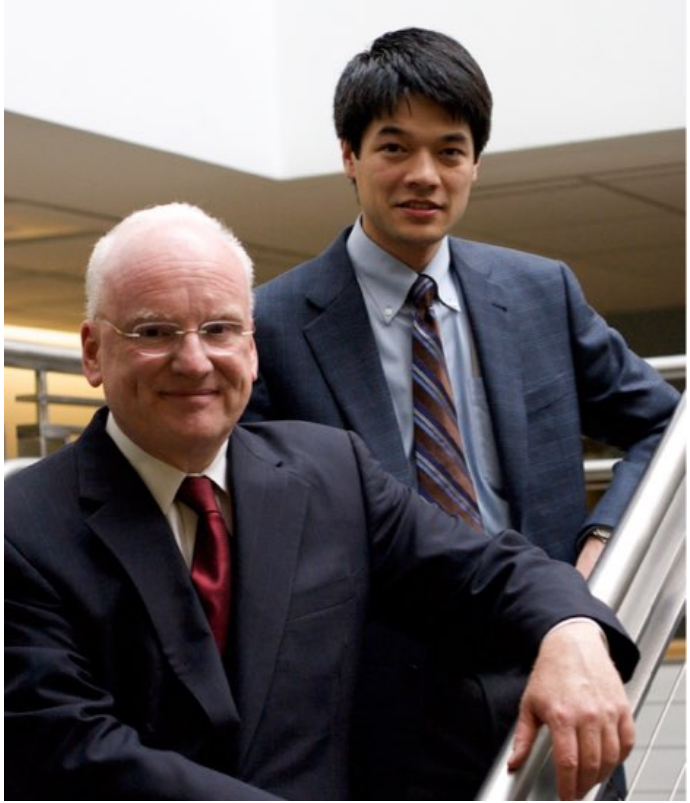
“The missing pieces of the three 21st century wars: Iraq, Afghanistan and Cyberspace”

Richard Clarke

Former White House Cybersecurity Czar

April 2, 2009 Distinguished Lecture

https://vimeo.com/23769166



Today: Cyber War

- Organized crime? Nation states?
- Big breaches
  - Target Breach
  - RSA breach
  - IRS breach
  - OPM breach
- Cyberphysical destruction: Stuxnet
- Your questions

March 17 – March 23, 2014 | businessweek.com

Bloomberg Businessweek

Fask Target

Exclusive
The biggest hack in retail history could have been prevented. So why didn't the company act?
p12

$5.99
12

A BIG BULLSEYE

Target is investigating a security breach that began the day before Thanksgiving, involving stolen credit and debit card information of millions of its retail customers.

About the retailer

Opened 1962 in Minneapolis

Online E-commerce site launched in 1999

Employees 361,000 worldwide

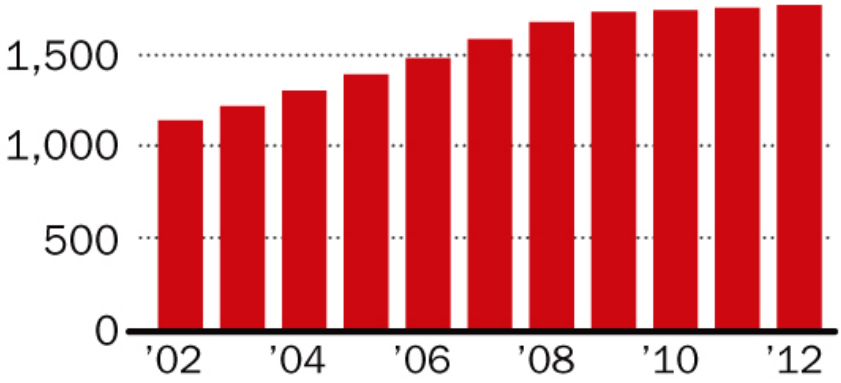
Gross profit $22.73 billion

Chairman, President, CEO
Gregg Steinhafel

Popularity No. 2 discount chain (behind Wal-Mart) in the U.S.

Stores 1,797 in 49 U.S. states; 124 in Canada

Number of stores



SOURCE: Target Corp., Hoovers, Yahoo Finance

MCT

TARGET

Nov. 27
Criminals gained access to customer information

Dec. 15
Target identified breach, resolved the issue

40 million
Names, credit, debit card numbers, expiration dates, three-digit security codes stolen

Data can be sold on the black market; used to create counterfeit cards

BUSINESS DAY

Target's Chief Information Officer Resigns

By THE ASSOCIATED PRESS MARCH 5, 2014

Beth M. Jacob had been vice president of Target Technology Services and chief information officer since 2008. Target

Two More Months Later…

BUSINESS DAY

Faltering Target Parts Ways With Chief

By ELIZABETH A. HARRIS MAY 5, 2014

Mr. Steinhafel's resignation is the latest in a series of moves made by the company as it struggles to recover from last year's holiday data breach. Keith Bedford/Reuters

APTS
ADVANCED PERSISTENT THREATS

Security Dynamics acquired RSA in 1996, kept company name RSA

BUSINESS DAY

RSA Faces Angry Users After Breach

By NELSON D. SCHWARTZ and CHRISTOPHER DREW JUNE 7, 2011

Email

Share

Tweet

Save

More

The nation's biggest banks and large technology companies like SAP rushed Tuesday to accept RSA Security's offer to replace their ubiquitous SecurID tokens as many computer security experts voiced frustration with the company.

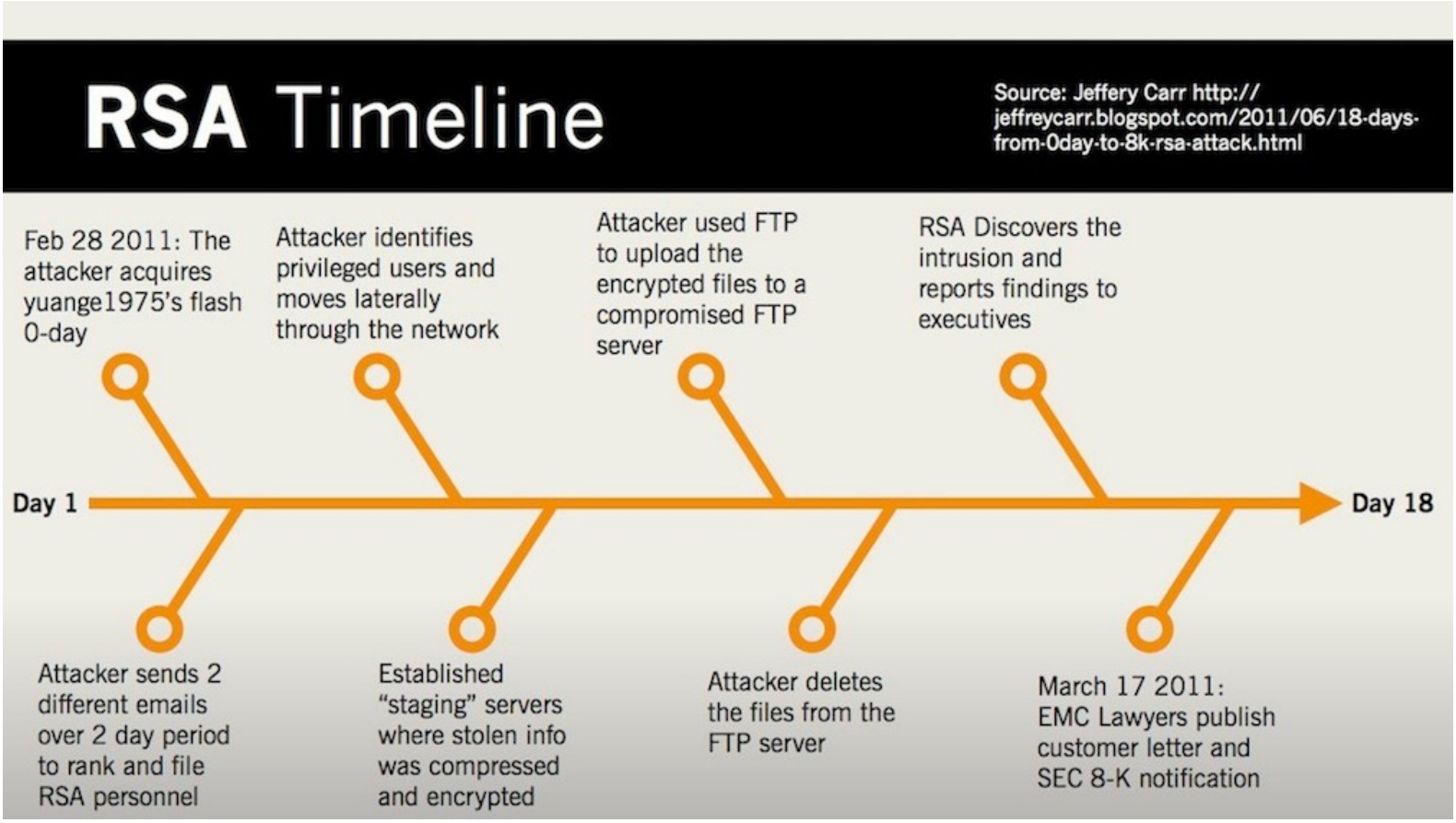
The company's admission of the RSA tokens' vulnerability on Monday was a shock to many customers because it came so long after a hacking attack on RSA in March and one on Lockheed Martin last month. The concern of customers and consultants over the way RSA, a unit of the tech giant EMC, communicated also raises the possibility that many customers will seek alternative solutions to safeguard remote access to their computer networks.

Bank of America, JPMorgan Chase, Wells Fargo and Citigroup said they planned to replace the tokens as soon as possible. The banks declined to say how many customers would be affected, although SAP said that most of its 50,000 employees used RSA's tokens and that it was seeking to replace them all.

Defense industry officials said Tuesday that concerns about the tokens had prompted some of the nation's largest military contractors to accelerate their plans to shift to computer smart cards and other emerging security technology.

Spear phishing

0-day flash exploit in Excel



http://blogs.rsa.com/anatomy-of-an-attack/

Art Coviello vigorously defended crypto researchers in the 2000s

Open Letter to RSA SecurID Customers

Arthur W. Coviello, Jr.

To Our Customers:

On March 17, 2011, RSA publicly disclosed that it had detected a very sophisticated cyber attack on its systems, and that certain information related to the RSA SecurID® product had been extracted. We immediately published best practices and our prioritized remediation steps, and proactively reached out to thousands of customers to help them implement those steps. We remain convinced that customers who implement these steps can be confident in their continued security, and customers in all industries have given us positive feedback on our remediation steps.

Certain characteristics of the attack on RSA indicated that the perpetrator's most likely motive was to obtain an element of security information that

RSA's Coviello breaks keynote script, takes on NSA controversy

CEO pivots discussion to industry rallying cry, invokes memory of JFK

By John Fontana for Identity Matters | February 25, 2014 -- 19:09 GMT (11:09 PST) | Topic: Security

RSA CEO Art Coviello abandoned his scheduled keynote presentation on identity at the company's flagship conference Tuesday to address the simmering controversy involving his security company and its alleged collaboration with the NSA .

His presentation, however, included little defense of RSA. The company said in December that it "categorically denies the allegations" that it took $10 milion from the NSA to provide a backdoor into its security software.

EECS 475
Introduction to Cryptography
Winter 2014

Home | Schedule | Handouts | Links

Announcements

First lecture on Wednesday, January 8, 2014.
Regarding weather, see note on Piazza after setting up an account.
No discussion sections or office hours held this first wintery week.

There are presently no open seats. Wait listed students must attend discussion and submit homework on-time in order to be considered if other students drop.

TECHNOLOGY

Cyberattack Exposes I.R.S. Tax Returns

By JADA F. SMITH MAY 26, 2015

The I.R.S. building in Washington. The agency said that criminals had been able to view thousands of tax returns.
Drew Angerer for The New York Times

WASHINGTON — Criminals used stolen data to gain access to past tax returns of more than 100,000 people through an application on the Internal Revenue Service's website, the agency said on Tuesday.

Using Social Security numbers, birth dates, street addresses and other personal information obtained elsewhere, the criminals completed a multistep authentication process and requested the tax returns and other filings, the I.R.S. said. Information from those forms was used to file fraudulent returns, the I.R.S. said, and the agency sent nearly $50 million in refunds before it detected the scheme.

"We're confident that these are not amateurs," John Koskinen, the I.R.S. commissioner, said. "These actually are organized crime syndicates that not only we but everybody in the financial industry are dealing with."

Hacking of Tax Returns More Extensive Than First Reported, I.R.S. Says

By MICHAEL S. SCHMIDT AUG. 17, 2015

The Internal Revenue Service headquarters in Washington. Hackers used information from returns to file fraudulent claims, generating nearly $50 million in refunds. J. David Ake/Associated Press

WASHINGTON — The Internal Revenue Service said Monday that hackers had gained access to the tax returns of more than 300,000 people, a far higher number than the agency had reported previously.

In the coming days, the I.R.S. will send 220,000 letters to taxpayers whose returns were probably viewed by the hackers, the agency said.

The agency had said in May that criminals using stolen data gained access to tax returns for 114,000 people through software called "Get Transcript" that allows taxpayers to retrieve their returns from previous years.

Relying on personal information — like Social Security numbers, birth dates and street addresses — the hackers got through a multistep authentication process. They then used information from the returns to file fraudulent ones, generating nearly $50 million in refunds.

"This breach is not just about what this single group is going to do with the information, but what happens when this information gets sold on the black market," said Peter Warren Singer, the author of "Cybersecurity and Cyberwar: What Everyone Needs to Know." "It's rare for the actual attackers to turn the information directly into money. They're stealing the data and selling it off to other people."

Peter Singer

Blue & Maize

I.R.S. Data Breach May Be Sign of More Personalized Schemes

By PATRICIA COHEN MAY 27, 2015

Budget cuts have left the I.R.S. struggling to prevent identity theft and refund fraud.
Andrew Harrer/Bloomberg, via Getty Images

The plot to steal information on 100,000 taxpayers from the Internal Revenue Service and hijack nearly $50 million in refunds not only reveals a previous security breach but hints at a wider fraud that may bedevil Americans in the future.

Some security and tax experts warned that this latest data theft might be a prelude to more targeted schemes aimed at duping taxpayers into handing millions of dollars over to criminals or to help thieves circumvent the agency's security filters next year and beyond.

The IRS Data Breach: Steps to Protect Americans' Personal Information

Full Committee Hearing

June 02, 2015 02:00PM

Location: SD-342, Dirksen Senate Office Building

U.S. Senate Committee on HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

Blue & Maize

Member Statements

Chairman Ron Johnson R (WI)
Download Statement (125.6 KB)

Senator Thomas R. Carper D (DE)
Download Statement (31.9 KB)

Witnesses

Panel I

Michael Kasper
Poughkeepsie, New York
Download Testimony (76.6 KB)

Kevin Fu, Ph.D.
Associate Professor
Department of Electrical Engineering and Computer Science, University of Michigan
Download Testimony (635 KB)

Jeffrey E. Greene
Director, Government Affairs North America
Symantec Corporation
Download Testimony (1.02 MB)

Panel II

The Honorable John A. Koskinen
Commissioner
Internal Revenue Service, U.S. Department of Treasury
Download Testimony (39.5 KB)

Terence V. Millholland
Chief Technology Officer
Internal Revenue Service, U.S. Department of Treasury

http://www.hsgac.senate.gov/hearings/the-irs-data-breach-steps-to-protect-americans-personal-information

OPM Director Rejects Blame for Breach

BITSIGHT

Panel Chair Laments 'No Clear Lines of Accountability'

Eric Chabrow (GovInfoSecurity) • June 23, 2015

OPM Director Katherine Archuleta testifies before a Senate panel.

The director of the Office of Personnel Management says neither she nor anyone else at OPM should be held personally responsible for a **data breach** of agency computers in which the personal information of millions of current and former government employees was stolen.

Hackers May Have Obtained Names of Chinese With Ties to U.S. Government

By **DAVID E. SANGER** and **JULIE HIRSCHFELD DAVIS** JUNE 10, 2015

The Office of Personnel Management building in Washington. The names of Chinese relatives, friends and frequent associates of American diplomats and other government officials may be in the hands of Chinese hackers.

Gary Cameron/Reuters

POLITICS

White House Weighs Sanctions After Second Breach of a Computer System

By MICHAEL D. SHEAR and SCOTT SHANE JUNE 12, 2015

ASIA PACIFIC

U.S. Decides to Retaliate Against China's Hacking

点击查看本文中文版 | Read in Chinese

By DAVID E. SANGER JULY 31, 2015

Email

Share

Tweet

Save

More

The Obama administration has determined that it must retaliate against China for the theft of the personal information of more than 20 million Americans from the databases of the Office of Personnel Management, but it is still struggling to decide what it can do without prompting an escalating cyberconflict.

The decision came after the administration concluded that the hacking attack was so vast in scope and ambition that the usual practices for dealing with traditional espionage cases did not apply.

But in a series of classified meetings, officials have struggled to choose among options that range from largely symbolic responses — for example, diplomatic protests or the ouster of known Chinese agents in the United States — to more significant actions that some officials fear could lead to an escalation of the hacking conflict between the two countries.

Group Exercise: What would you do if you were the U.S. Cybersecurity Czar? The Chinese equivalent?

Attack Gave Chinese Hackers Privileged Access to U.S. Systems

By DAVID E. SANGER, NICOLE PERLROTH and MICHAEL D. SHEAR JUNE 20, 2015

Katherine Archuleta, director of the Office of Personnel Management, in Congress on Tuesday.
Cliff Owen/Associated Press

Email
Share
Tweet
Save
More

WASHINGTON — For more than five years, American intelligence agencies followed several groups of Chinese hackers who were systematically draining information from defense contractors, energy firms and electronics makers, their targets shifting to fit Beijing's latest economic priorities.

But last summer, officials lost the trail as some of the hackers changed focus again, burrowing deep into United States government computer systems that contain vast troves of personnel data, according to American officials briefed on a federal investigation into the attack and private security experts.

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

Cybersecurity

OPM director refuses to resign amid new hack revelations

By Zach Noble Jul 09, 2015

A mere half-hour after releasing the long-awaited official estimate of how many people had been exposed in the massive background investigation breach -- 21.5 million, higher than some previous unofficial estimates -- the Office of Personnel Management hosted a conference call for media that shed a bit more light on the situation.

In a call with reporters, OPM Director Katherine Archuleta said again that she would not resign over the security breaches.

In the brief and carefully controlled call, OPM Director Katherine Archuleta said she would not resign over the breaches.

When the first reporter asked about congressional calls for her resignation, Archuleta repeated her stock speech about how she had inherited a flawed legacy system and has worked "aggressively" to improve OPM's cybersecurity.

One Day Later

Katherine Archuleta, Director of Personnel Agency, Resigns

By JULIE HIRSCHFELD DAVIS JULY 10, 2015

Katherine Archuleta, the director of the Office of Personnel Management, at a Senate hearing last month. Ms. Archuleta resigned the post on Friday. Chip Somodevilla/Getty Images North America

ASIA PACIFIC

U.S. Fears Data Stolen by Chinese Hacker Could Identify Spies

By MARK MAZZETTI and DAVID E. SANGER JULY 24, 2015

WASHINGTON — American officials are concerned that the Chinese government could use the stolen records of millions of federal workers and contractors to piece together the identities of intelligence officers secretly posted in China over the years.

The potential exposure of the intelligence officers could prevent a large cadre of American spies from ever being posted abroad again, current and former intelligence officials said. It would be a significant setback for intelligence agencies already concerned that a recent data breach at the Office of Personnel Management is a major windfall for Chinese espionage efforts.

In the days after the breach of records of millions of federal workers and contractors became public last month, some officials in the Obama administration said that the theft was not as damaging as it might have been because the Chinese hackers did not gain access to the identities of American undercover spies.

ASIA PACIFIC

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says

By DAVID E. SANGER SEPT. 23, 2015

WASHINGTON — Just a day before the arrival of President Xi Jinping here for a meeting with President Obama that will be focused heavily on limiting cyberespionage, the Office of Personnel Management said Wednesday that the hackers who stole security dossiers from the agency also got the fingerprints of 5.6 million federal employees.

The attack on the agency, which is the main custodian of the government's most important personnel records, has been attributed to China by American intelligence agencies, but it is unclear exactly what group or organization engineered it. Before Wednesday, the agency had said that it lost only 1.1 million sets of fingerprints among the records of roughly 22 million individuals that were compromised.

So what exactly did the intruders get?

So it's even worse?

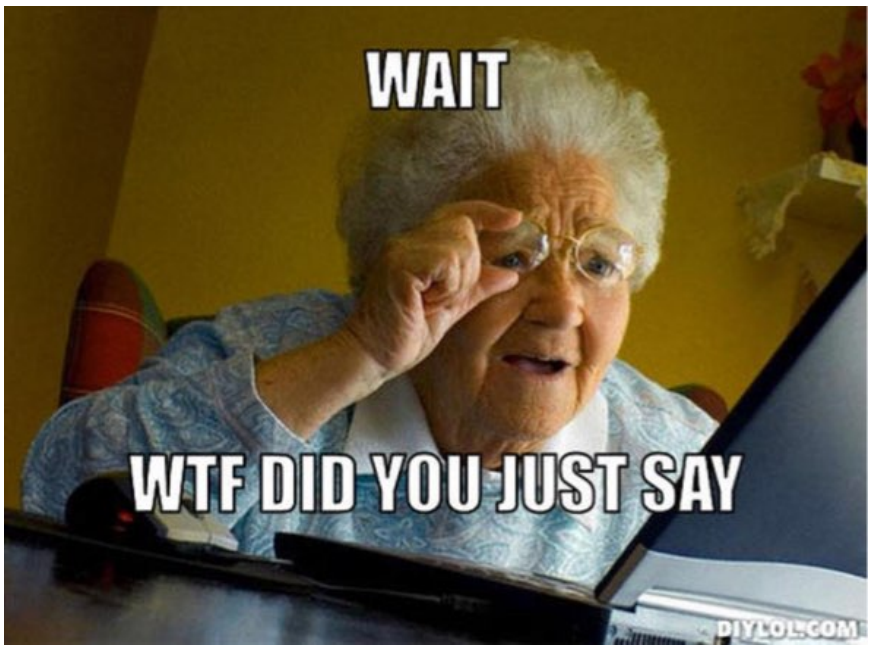
ASIA PACIFIC

China Calls Hacking of U.S. Workers' Data a Crime, Not a State Act

By MICHAEL FORSYTHE and DAVID E. SANGER DEC. 2, 2015

HONG KONG — China has acknowledged for the first time that the breach of the United States Office of Personnel Management's computer systems, which the Obama administration said exposed the personal information of more than 21.5 million people, was the work of Chinese hackers. But China insisted that the breach was the result of criminal activity, not a state-sponsored cyberattack.

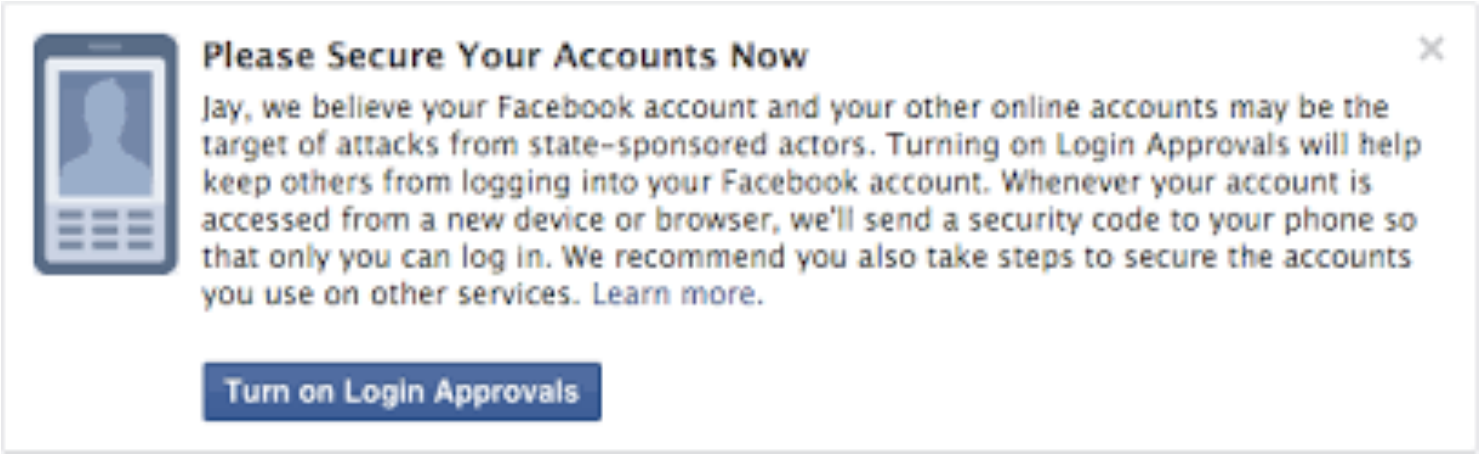
The assertion came in one paragraph midway through an article published Tuesday by Xinhua, the state-run news agency, about a meeting in Washington between top Chinese and American law enforcement officials, and it raised more questions than it answered.

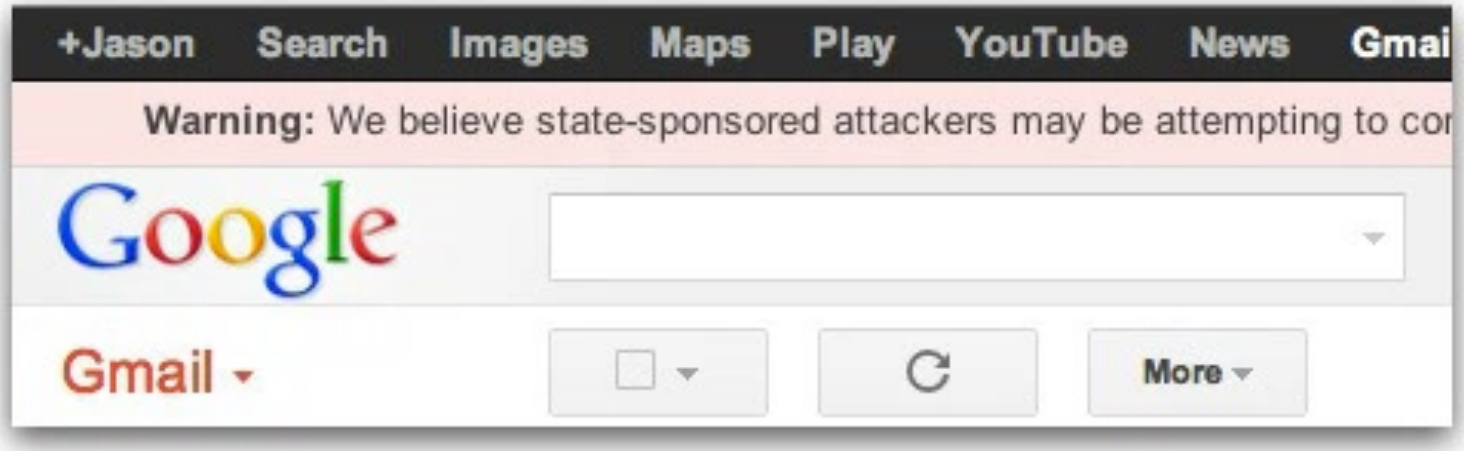


BRIAN BARRETT SECURITY 10.19.15 11:28 AM

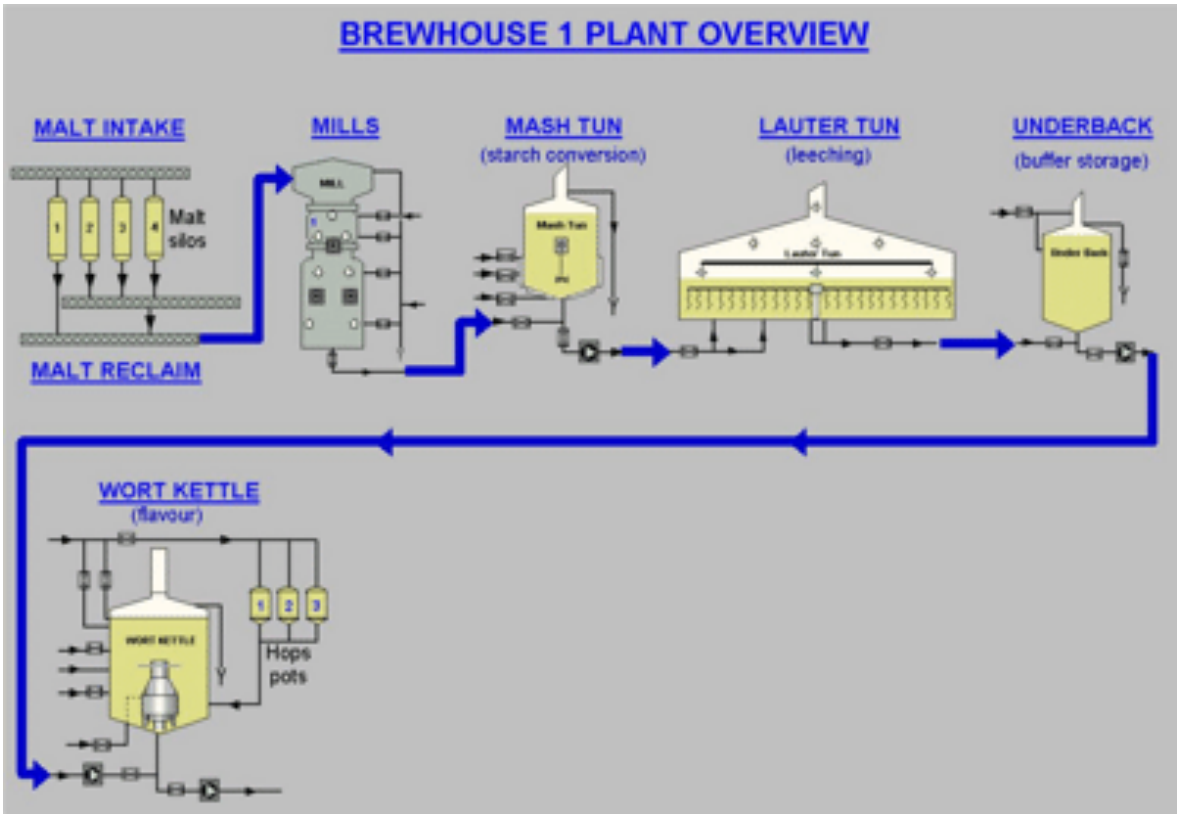
FACEBOOK NOW WARNS USERS OF STATE-SPONSORED ATTACKS

In 2012, Google began notifying its users if it believed those people's accounts or computers were at risk of a state-sponsored attack. Three years later, Facebook has now followed suit, the latest in a string of security-conscious measures the social network has recently enacted.

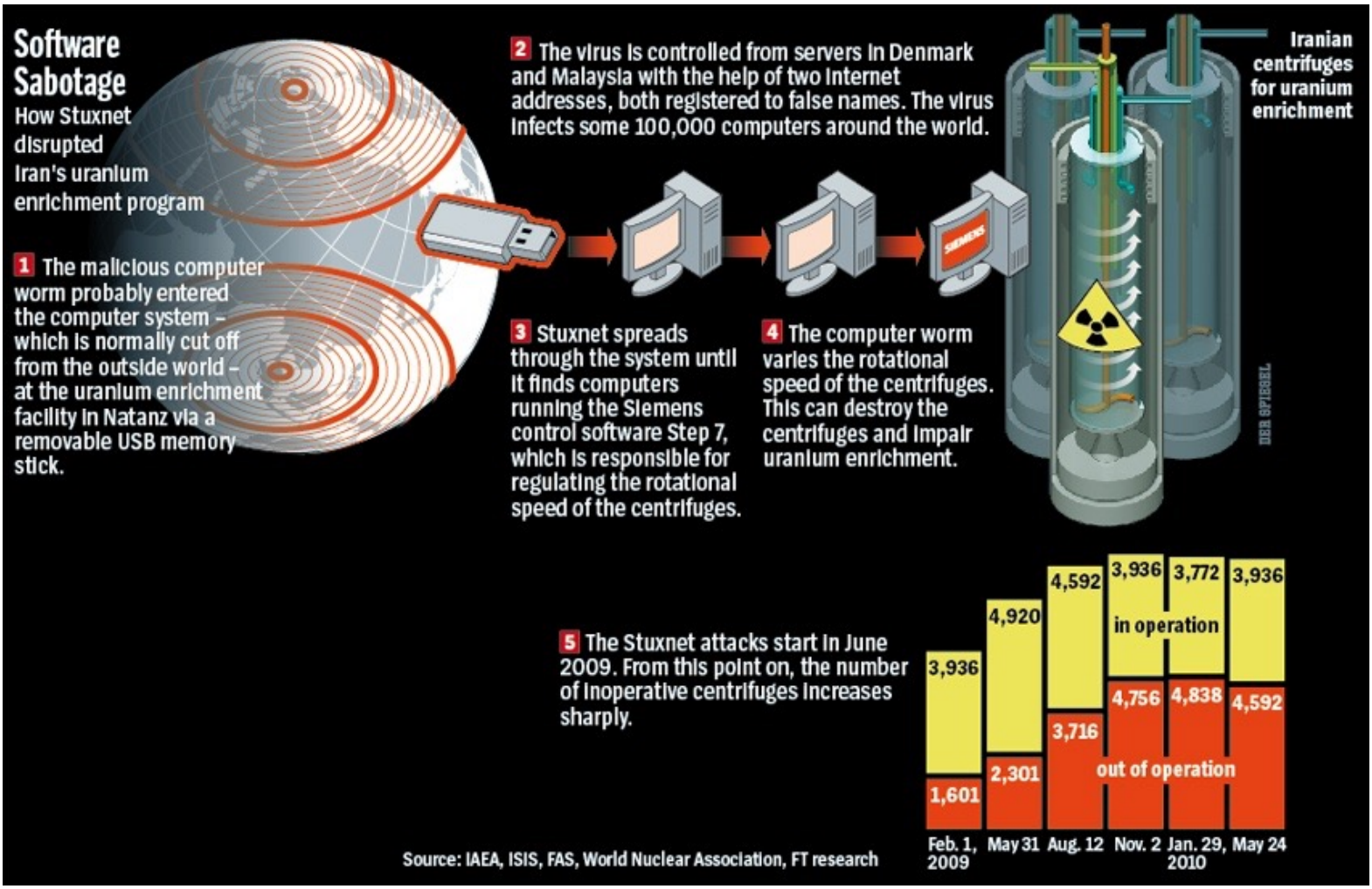




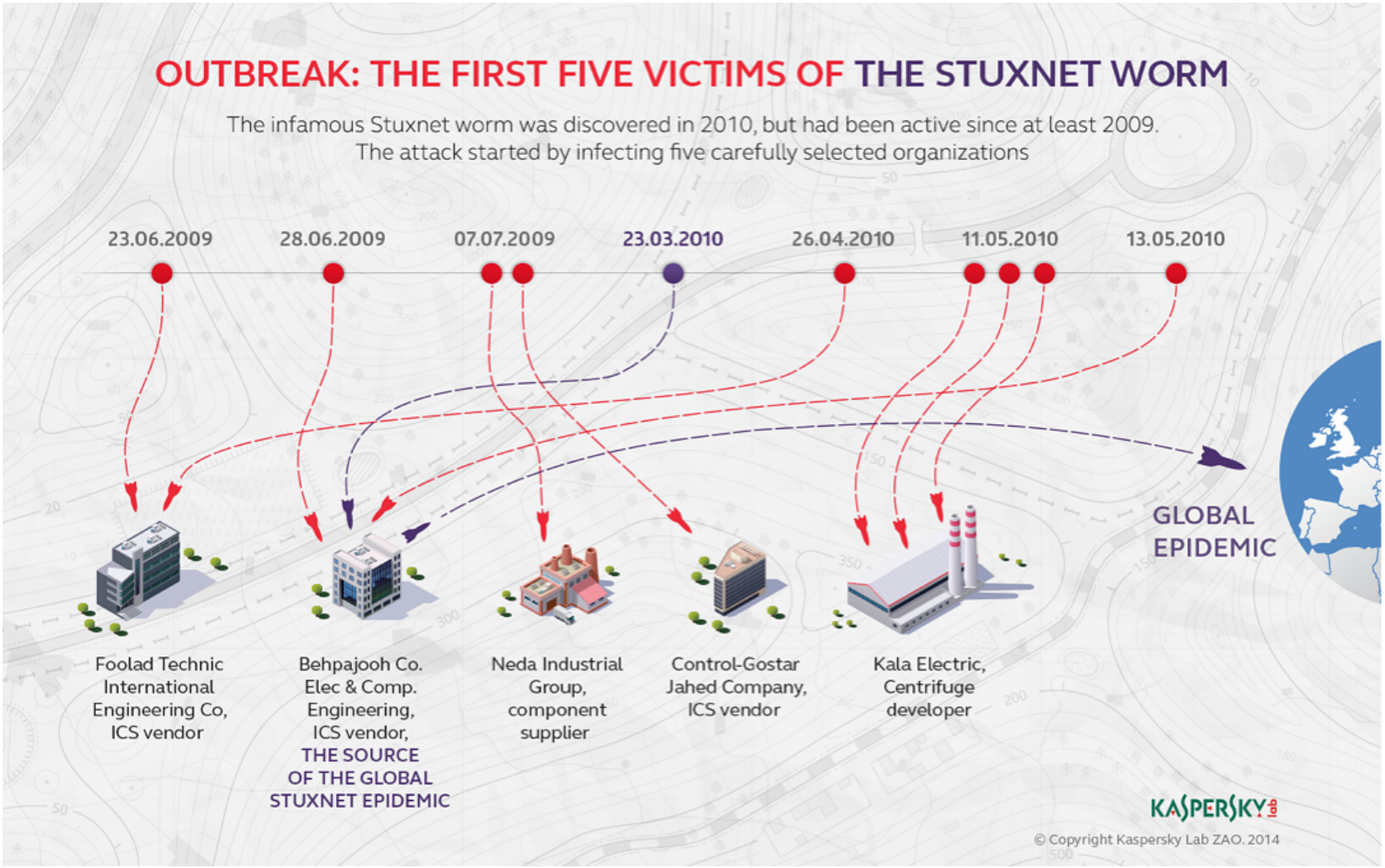
Stuxnet: That's not a beer brewery



http://www.futuristix.co.za/live/content.php?Item_ID=705
http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/



http://www.extremetech.com/computing/200898-windows-pcs-vulnerable-to-stuxnet-attack-five-years-after-patches




FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE
인터뷰 INTERVIEW 인터뷰
FALL

MEDIA

Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm

By MICHAEL CIEPLY and BROOKS BARNES DEC. 30, 2014

A Hollywood billboard for Sony Pictures' "The Interview" was removed on Dec. 18, after the studio canceled its theatrical run. Robyn Beck/Agence France-Presse — Getty Images

RELATED COVERAGE

'The Interview' Brings In $15 Million on Web DEC. 28, 2014

North Korea Accuses U.S. of Staging Internet Failure DEC. 27, 2014

LOS ANGELES — It was three days before Thanksgiving, the beginning of a quiet week for Sony Pictures. But Michael Lynton, the studio's chief executive, was nonetheless driving his Volkswagen GTI toward Sony's lot at 6 a.m. Final planning for corporate meetings in Tokyo was on his agenda — at least until his cellphone rang.

The studio's chief financial officer, David C. Hendler, was calling to tell his boss that Sony's computer system had been compromised in a hacking of unknown proportions. To prevent further damage, technicians were debating whether to take Sony Pictures entirely offline.

Shortly after Mr. Lynton reached his office in the stately Thalberg building at Sony headquarters in Culver City, Calif., it became clear that the situation was much more dire. Some of the studio's 7,000 employees, arriving at work, turned on their computers to find macabre images of Mr. Lynton's severed head. Sony shut down all computer systems shortly thereafter, including those in overseas offices, leaving the company in the digital dark ages: no voice mail, no corporate email, no production systems.

Shadow Brokers

Skype Vanishes From App Stores in China, Including Apple's

By PAUL MOZUR NOV. 21, 2017

An internet cafe in Beijing. China has long wielded the most sophisticated and comprehensive internet controls in the world. Roman Pilipey/European Pressphoto Agency

RELATED COVERAGE


China Block
Online Cens


Apple Remo
That Help Ir
JULY 29, 2017


China's New
Foreign Firn

Earlier this autumn, the Facebook-owned messaging service WhatsApp was hit by blockages in China, becoming the latest in a long line of products to be rendered unusable by Chinese government filters. Others include Gmail, Facebook, Snapchat, Twitter, Telegram and Line.

Beijing appears to have disabled these apps because they generally feature encryption options that make messages harder for the government to monitor. Such products also often run afoul of government rules that require the use of real-name identification for each and every account.

Lightweight reading for the holiday:

- Deep State by Ambinder & Grady (discusses OLYMPIC GAMES)
- Secrets and Lies by Bruce Schneier
- Computer Related Risks by Peter G. Neumann