02- Introduction to Security

Lujo Bauer, Nicolas Christin, and Abby Marsh

January 13, 2015

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

Plan for This Lecture

- Defining and motivating computer security
- Types of misuse
- Threats and attackers
- Basic security analysis

Goals: To learn…

- about the breadth of things that one needs to worry about
- how an attacker might think
- how to reason about the security of a system

What Is Computer Security?

- Protecting information systems against misuse and interference
- “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)

What Is Computer Security?

- Broadly comprised of three types of properties
  - *Confidentiality*: information is protected from unintended disclosure
    - Secrecy, privacy
  - *Integrity*: system and data are maintained in a correct and consistent condition
  - *Availability*: systems and data are usable when needed
    - Also includes timeliness
- These concepts overlap (and clash)
- These concepts are (perhaps) not all-inclusive
  - Spam?
  - “Non-business related” surfing?

Why Is Computer Security Important?

- Software / information systems are everywhere
- Software has bugs
- Attackers seek to exploit bugs

Exploiting Bugs as a Nuisence

- To be annoying
  - Newsday technology writer & hacker critic found …
    - Email box jammed with thousands of messages
    - Phone reprogrammed to an out of state number where caller's heard an obscenity-loaded recorded message

[Time Magazine, December 12, 1994]

Exploiting Bugs as a Nuisance

- MyDoom (2004) - $38.5 billon
- SoBig (2003) - $37.1 billion
- Love Bug (2000) - $15 billion
- Code Red (2001) - $2 billion

Exploiting Bugs for Profit

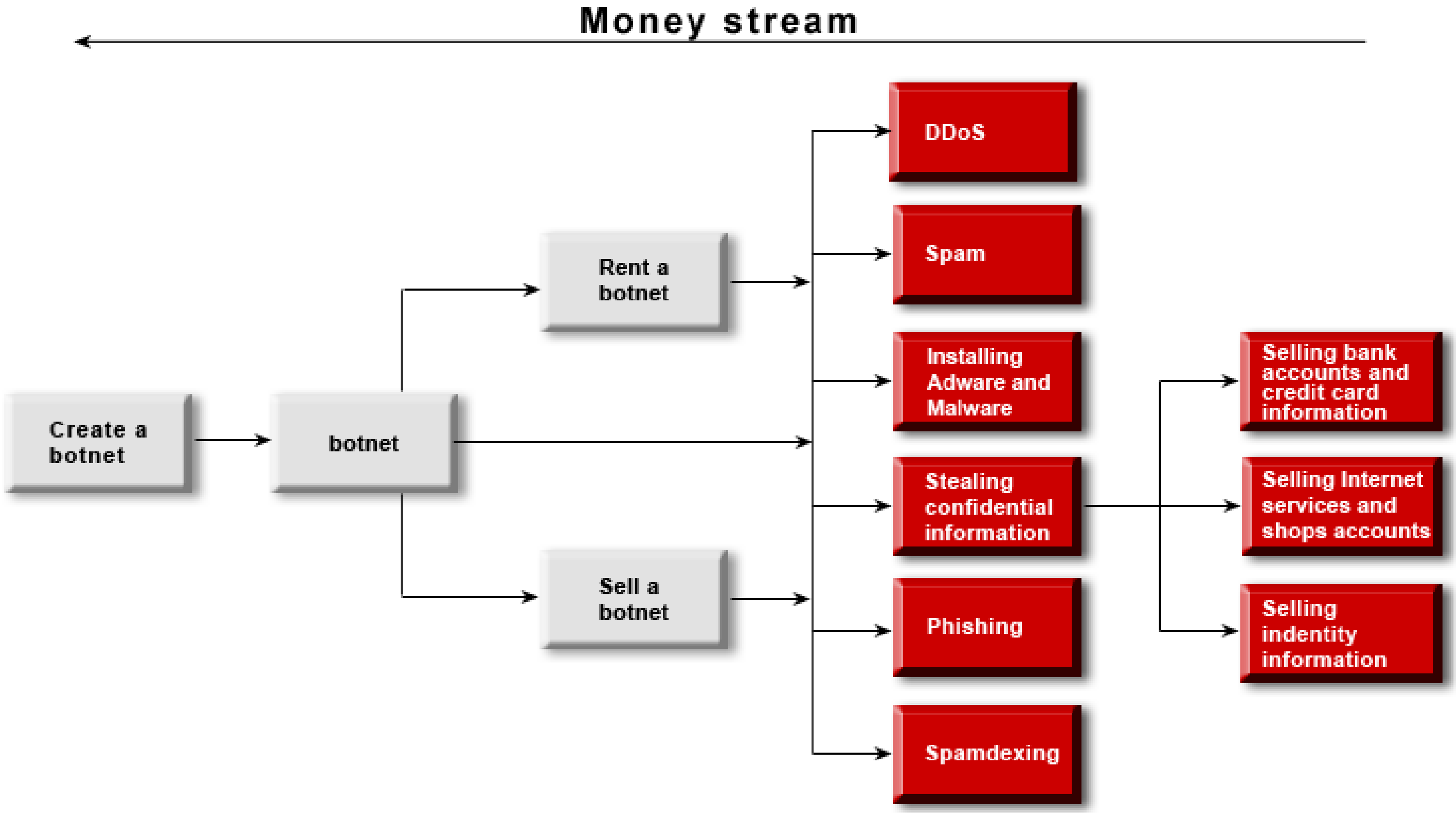
- Hacker convicted of breaking into a business' computer system, stealing confidential information and threatening disclosure if $200,000 not paid

[U.S. Dept. of Justice Press Release, Jul 2003]

- 11 people indicted for stealing more than 40 million credit card and debit card numbers

[CNN, Aug 2008]

The Economics of Botnets


Money stream
Create a botnet
botnet
Rent a botnet
Sell a botnet
DDoS
Spam
Installing Adware and Malware
Stealing confidential information
Phishing
Spamdexing
Selling bank accounts and credit card information
Selling Internet services and shops accounts
Selling indentity information

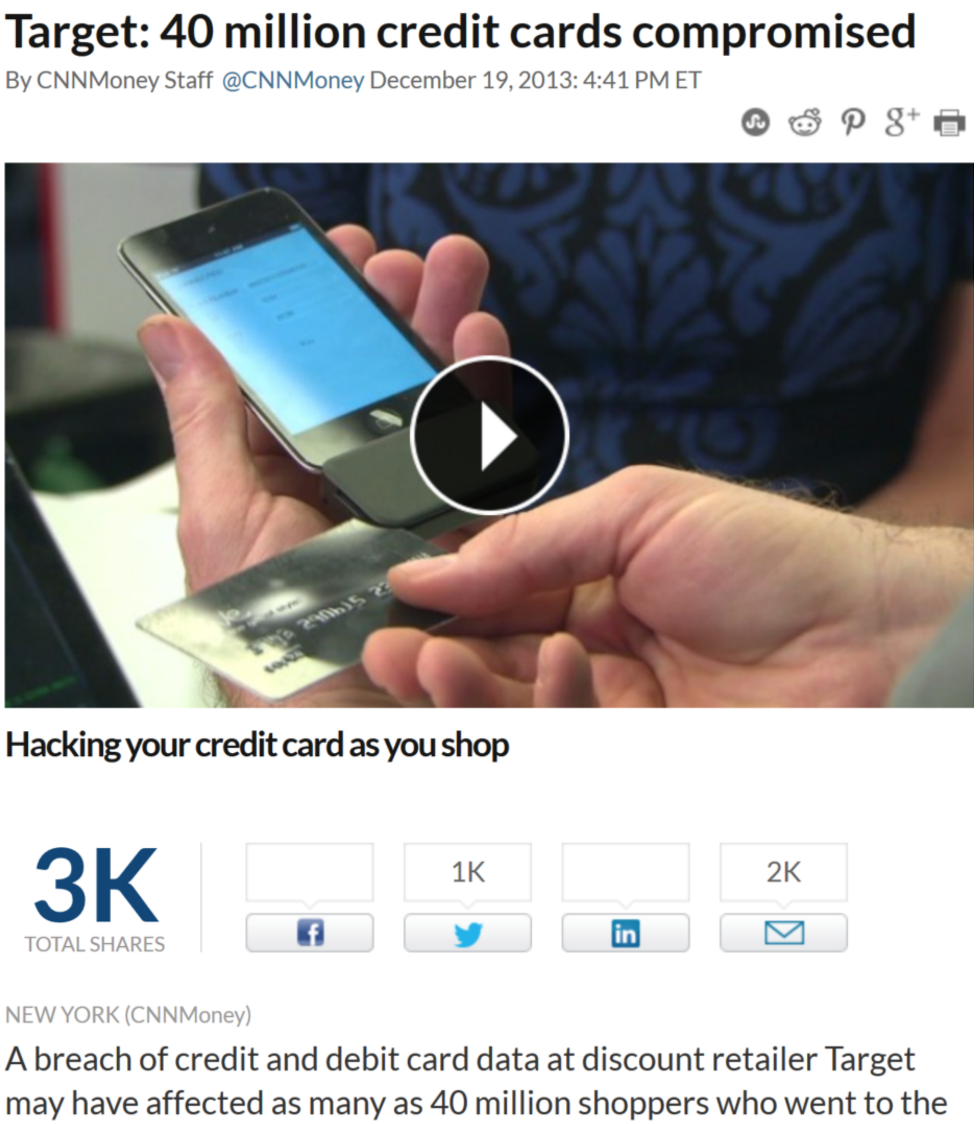
[Y. Namestnikov. The economics of botnets. Kaspersky Lab, 2009.]

Pricelists

- $100-180 per 1000 installs (2011)
- $1-1,500 stolen bank account details (2009)
- $20-100+ US credit card (2013)
- $5-8 US citizen personal data (2009)
- $7-15 user accounts for paid online services (2009)
- $1000-2000 per month for botnet spam services (2009)
- $50-$$$ per day for botnet DDoS services (2009)
- $125,000 for zero-day browser exploit to private party (2012)
- $250,000 for zero-day iOS exploit to government (2012)

Sources:

- Andy Greenberg. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. *Forbes*, 23 Mar 2012.
- Juan Caballero, Chris Grier, Christian Kreibich, and Vern Paxon. Measuring pay-per-install: the commoditization of malware distribution. In *Proc. USENIX Security*, 2011.
- Kaspersky reveals price list for botnet attacks. *Computer Weekly*, 23 Jul 2009.
- Stolen Target credit cards and the black market. *Tripwire*, 21 Dec 2013.



Target: 40 million credit cards compromised

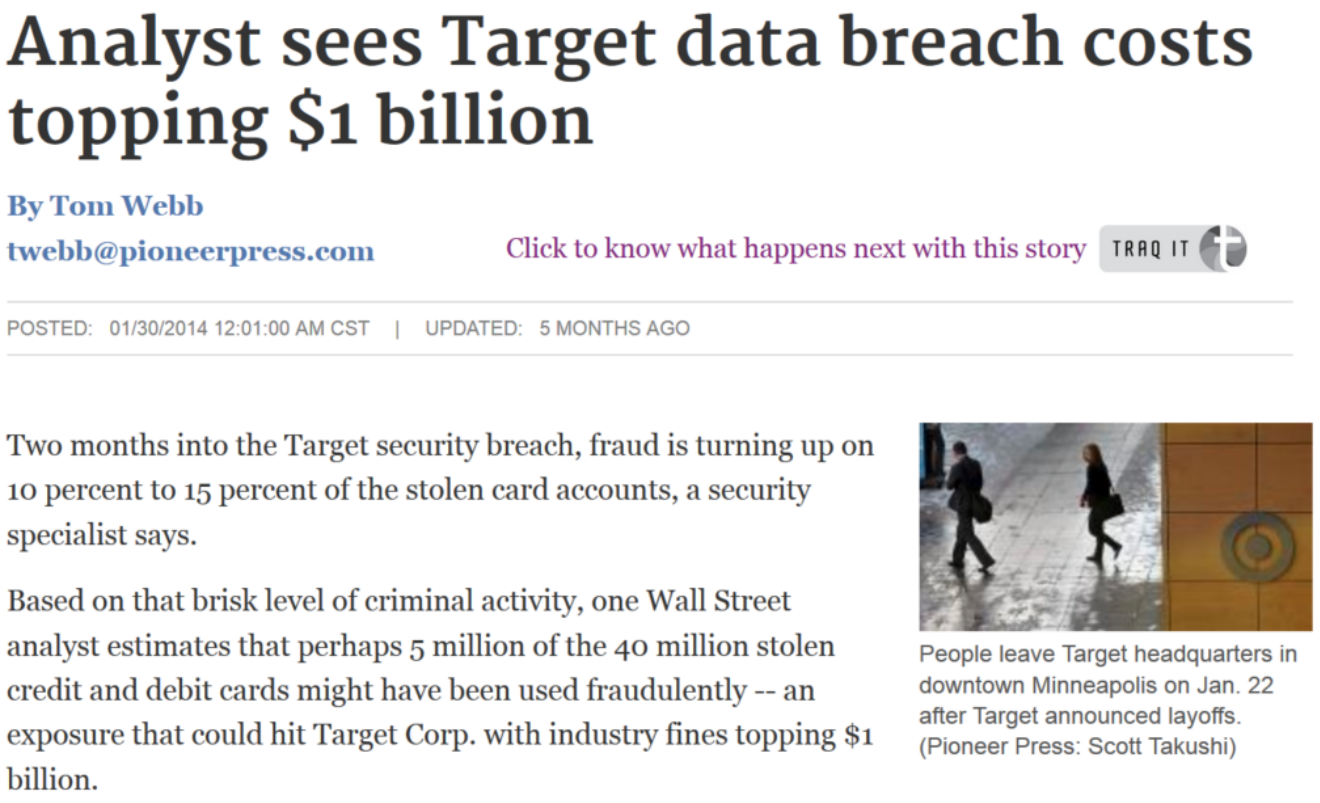
By CNNMoney Staff @CNNMoney December 19, 2013: 4:41 PM ET

Hacking your credit card as you shop

NEW YORK (CNNMoney)

A breach of credit and debit card data at discount retailer Target may have affected as many as 40 million shoppers who went to the

[CNN.com, Dec 19, 2013 http://money.cnn.com/2013/12/18/news/companies/target-credit-card/]



Analyst sees Target data breach costs topping $1 billion

By Tom Webb
twebb@pioneerpress.com

Click to know what happens next with this story TRAQ IT

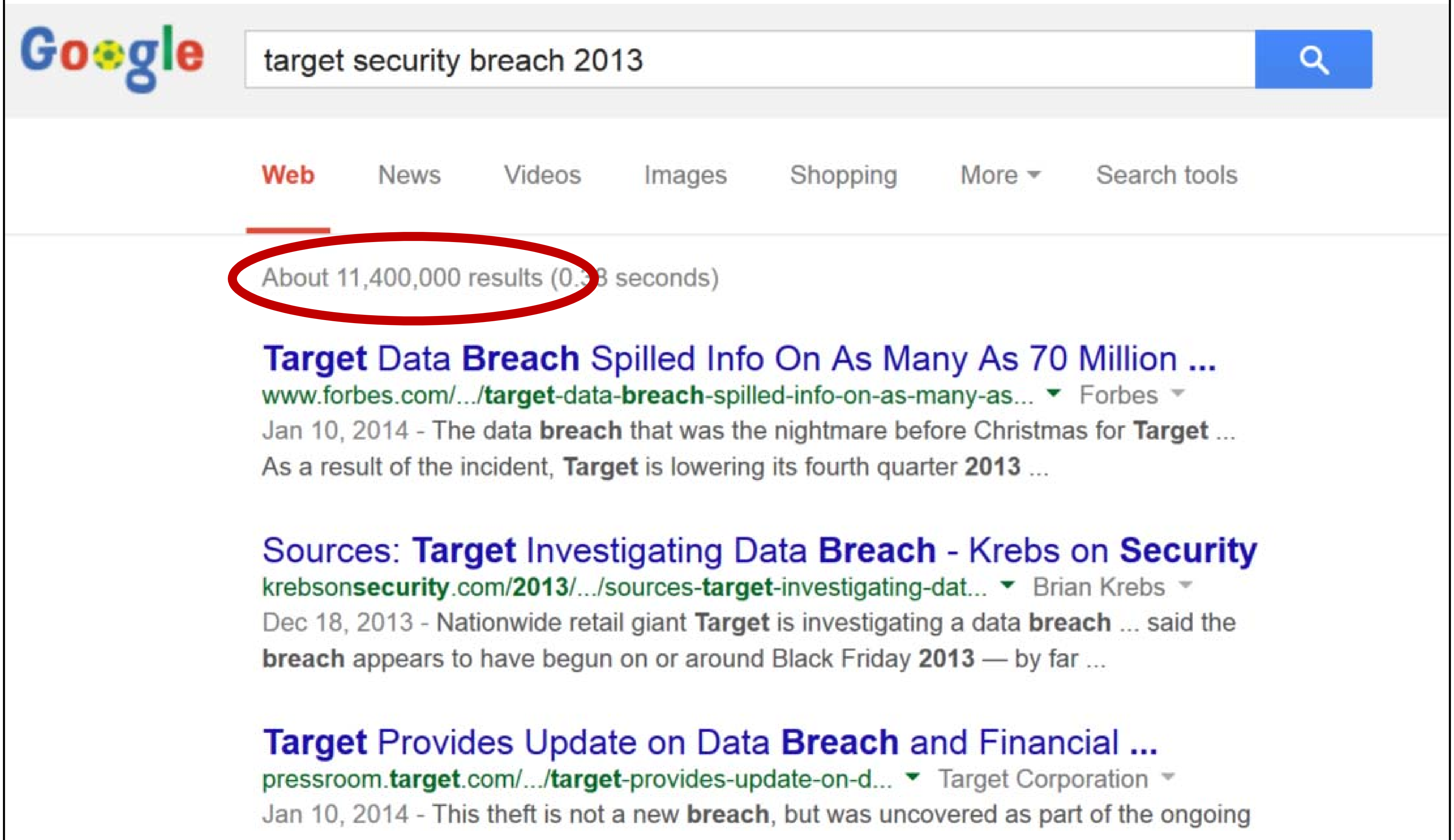
POSTED: 01/30/2014 12:01:00 AM CST | UPDATED: 5 MONTHS AGO

Two months into the Target security breach, fraud is turning up on 10 percent to 15 percent of the stolen card accounts, a security specialist says.

Based on that brisk level of criminal activity, one Wall Street analyst estimates that perhaps 5 million of the 40 million stolen credit and debit cards might have been used fraudulently -- an exposure that could hit Target Corp. with industry fines topping $1 billion.

People leave Target headquarters in downtown Minneapolis on Jan. 22 after Target announced layoffs. (Pioneer Press: Scott Takushi)

[Pioneer Press, January 30, 2014 http://www.twincities.com/ci_25029900]



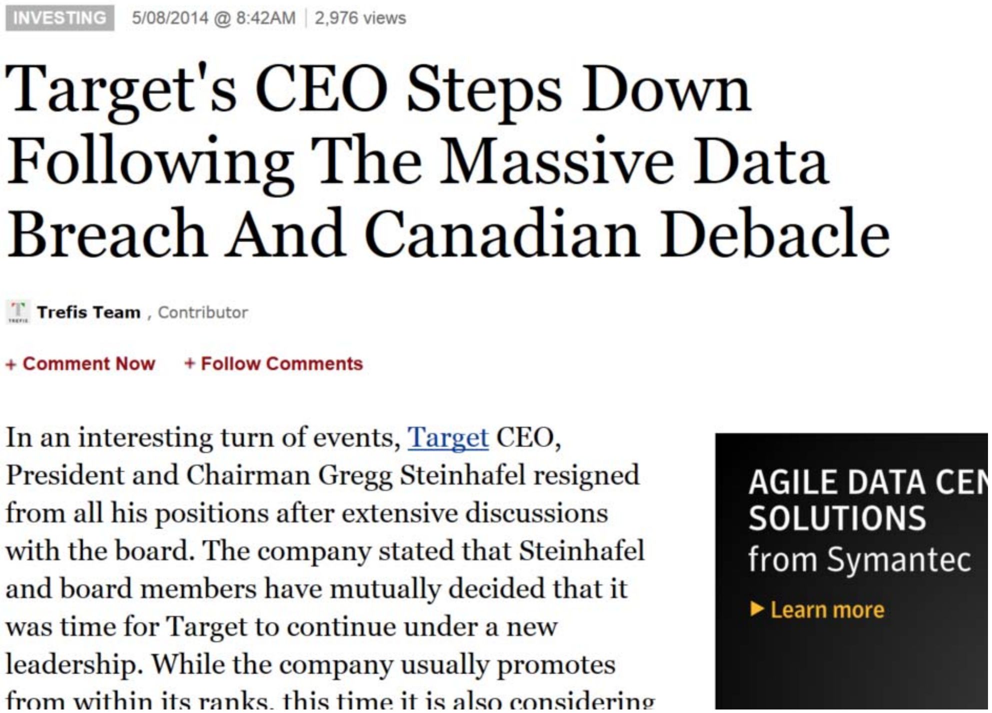
target security breach 2013

About 11,400,000 results (0.38 seconds)

Target Data **Breach** Spilled Info On As Many As 70 Million ...
www.forbes.com/.../**target**-data-**breach**-spilled-info-on-as-many-as... Forbes
Jan 10, 2014 - The data **breach** that was the nightmare before Christmas for **Target** ...
As a result of the incident, **Target** is lowering its fourth quarter **2013** ...

Sources: **Target** Investigating Data **Breach** - Krebs on **Security**
krebson**security**.com/**2013**/.../sources-**target**-investigating-dat... Brian Krebs
Dec 18, 2013 - Nationwide retail giant **Target** is investigating a data **breach** ... said the
breach appears to have begun on or around Black Friday **2013** — by far ...

Target Provides Update on Data **Breach** and Financial ...
pressroom.**target**.com/.../**target**-provides-update-on-d... Target Corporation
Jan 10, 2014 - This theft is not a new **breach**, but was uncovered as part of the ongoing



INVESTING 5/08/2014 @ 8:42AM | 2,976 views

Target's CEO Steps Down Following The Massive Data Breach And Canadian Debacle

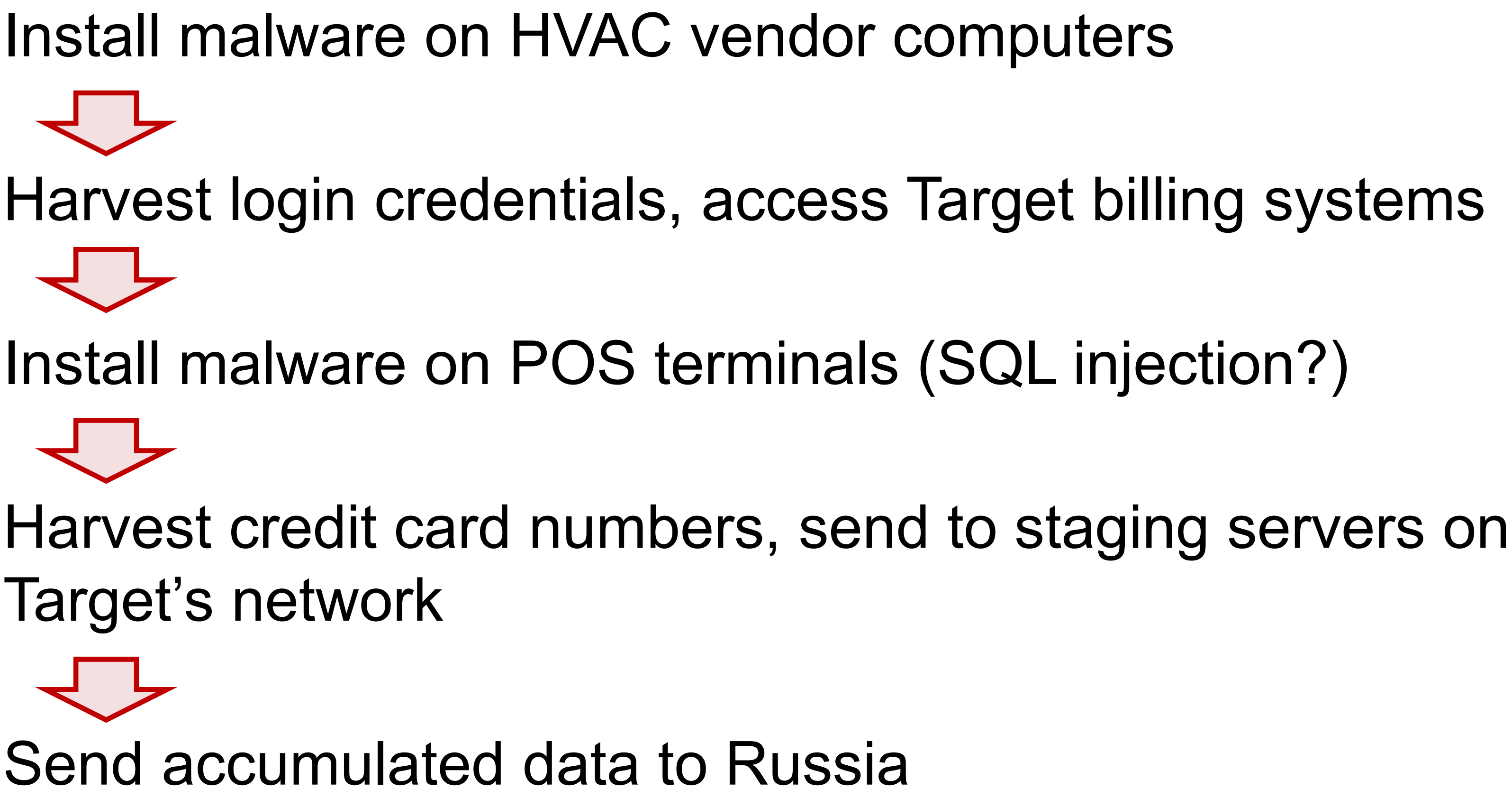
Trefis Team , Contributor

+ Comment Now + Follow Comments

In an interesting turn of events, Target CEO, President and Chairman Gregg Steinhafel resigned from all his positions after extensive discussions with the board. The company stated that Steinhafel and board members have mutually decided that it was time for Target to continue under a new leadership. While the company usually promotes from within its ranks, this time it is also considering

[Forbes, May 8, 2014 http://www.forbes.com/sites/greatspeculations/2014/05/08/targets-ceo-steps-down-following-the-massive-data-breach-and-canadian-debacle/]

Target Breach – What Happened?



Install malware on HVAC vendor computers

Harvest login credentials, access Target billing systems

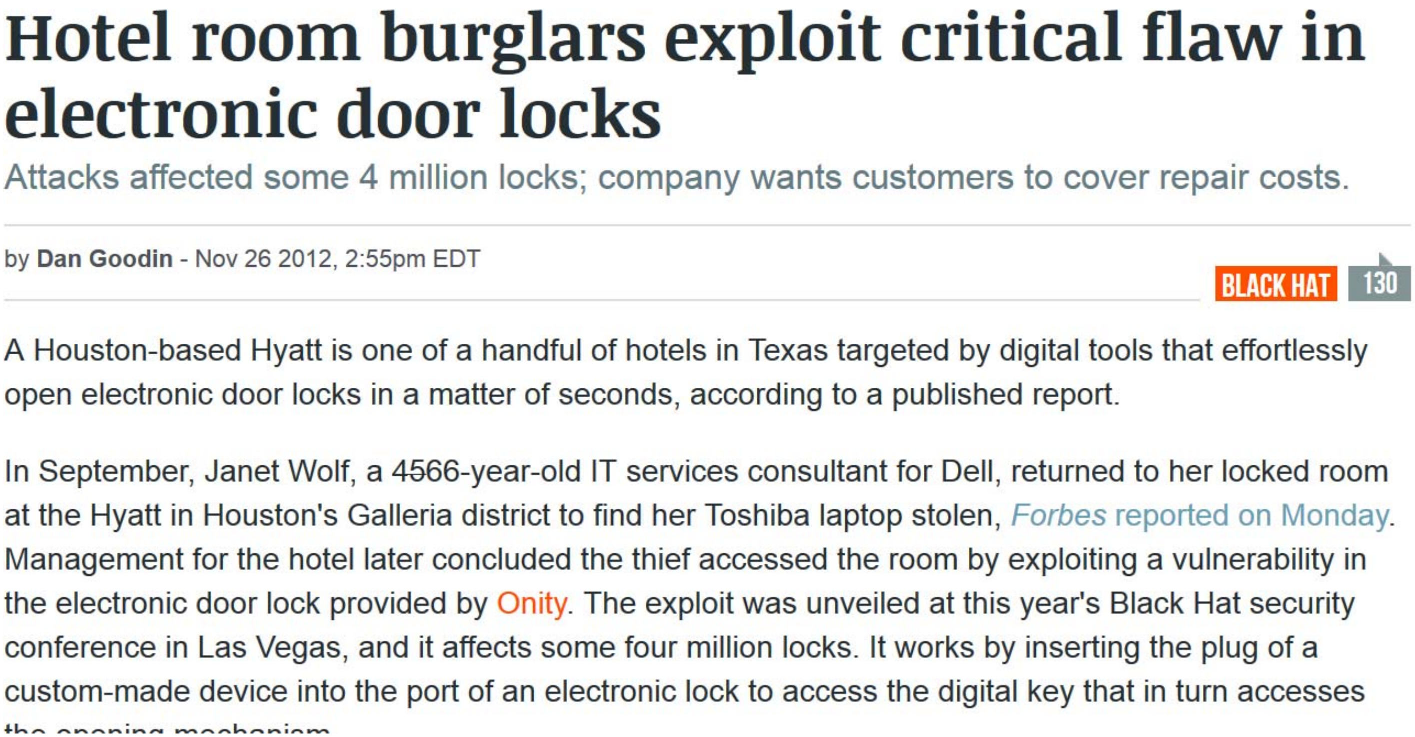
Install malware on POS terminals (SQL injection?)

Harvest credit card numbers, send to staging servers on Target’s network

Send accumulated data to Russia

Target Breach – Lessons

- With security, can’t just go through the motions
  - 300 information security staff
  - $1.6M malware detection system
- Be prepared to react (defense + response)
- Attacks are sometimes built from small steps
- Use least privilege, separation
  - Billing systems have no business accessing POS terminals
- Partners’ systems are a liability
  - Poor anti-virus, training
- Don’t forget the human element
  - Attack started with phishing emails



Hotel room burglars exploit critical flaw in electronic door locks

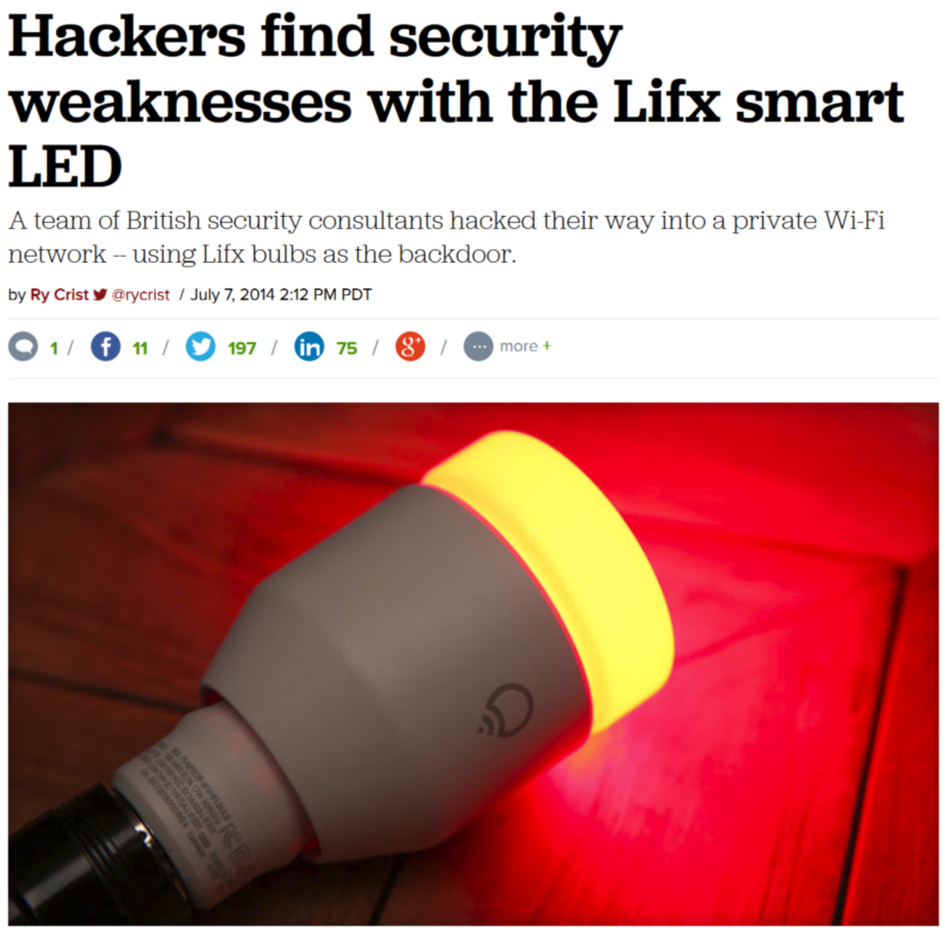
Attacks affected some 4 million locks; company wants customers to cover repair costs.

by **Dan Goodin** - Nov 26 2012, 2:55pm EDT

A Houston-based Hyatt is one of a handful of hotels in Texas targeted by digital tools that effortlessly open electronic door locks in a matter of seconds, according to a published report.

In September, Janet Wolf, a ~~45~~66-year-old IT services consultant for Dell, returned to her locked room at the Hyatt in Houston's Galleria district to find her Toshiba laptop stolen, *Forbes* reported on Monday. Management for the hotel later concluded the thief accessed the room by exploiting a vulnerability in the electronic door lock provided by Onity. The exploit was unveiled at this year's Black Hat security conference in Las Vegas, and it affects some four million locks. It works by inserting the plug of a custom-made device into the port of an electronic lock to access the digital key that in turn accesses the opening mechanism

[ars technica, Nov 26, 2012 http://arstechnica.com/security/2012/11/hotel-room-burglars-exploit-critical-flaw-in-electronic-door-locks/]



Hackers find security weaknesses with the Lifx smart LED

A team of British security consultants hacked their way into a private Wi-Fi network -- using Lifx bulbs as the backdoor.

by Ry Crist @rycrist / July 7, 2014 2:12 PM PDT

[Ry Crist, CNET, July 7, 2014 http://www.cnet.com/news/hackers-discover-security-weaknesses-within-the-lifx-smart-led/]

Types of Information System Misuse (1)

[Neumann and Parker 1989]

- External

Visual spying	Observing keystrokes or screens
Misrepresentation	Deceiving operators and users
Physical scavenging	“Dumpster diving” for printouts

- Hardware misuse

Logical scavenging	Examining discarded/stolen media
Eavesdropping	Intercepting electronic or other data
Interference	Jamming, electronic or otherwise
Physical attack	Damaging or modifying equipment
Physical removal	Removing equipment & storage media

Types of Information System Misuse (2)

[Neumann and Parker 1989]

- Masquerading

– Impersonation	Using false identity external to computer
– Piggybacking	Usurping workstations, communication
– Spoofing	Using playback, creating bogus systems
– Network weaving	Masking physical location or routing

- Pest programs

– Trojan horses	Implanting malicious code
– Logic bombs	Setting time or event bombs
– Malevolent worms	Acquiring distributed resources
– Viruses	Attaching to programs and replicating

- Bypasses

– Trapdoor attacks	Utilizing existing flaws
– Authorization attacks	Password cracking

Types of Information System Misuse (3)

[Neumann and Parker 1989]

• Active misuse	
– Basic	Creating false data, modifying data
– Denials of service	Saturation attacks
• Passive misuse	
– Browsing	Making random or selective searches
– Inference, aggregation	Exploiting traffic analysis
– Covert channels	Covert data leakage
• Inactive misuse	Failing to perform expected duties
• Indirect misuse	Breaking crypto keys

Basic Security Analysis

- How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. What are the security requirements?
4. What security approaches are effective?

1. What Are We Protecting?

- Enumerate assets and their value
- Understand architecture of system
- Useful questions to ask
  - What is the operating value, i.e., how much would we lose per day/hour/minute if the resource stopped?
  - What is the replacement cost? How long would it take to replace it?

2. Who Is the Adversary?

- Identify potential attackers
  - How motivated are they?
- Estimate attacker resources
  - Time and money
- Estimate number of attackers, probability of attack

Common (Abstract) Adversaries

- Attacker action
  - Passive attacker: eavesdropping
  - Active attacker: eavesdropping + data injection
- Attacker sophistication
  - Ranges from script kiddies to government-funded group of professionals
- Attacker access
  - External attacker: no knowledge of cryptographic information, no access to resources
  - Internal attacker: complete knowledge of all cryptographic information, complete access
    - Result of system compromise

3. What Are the Security Requirements?

- Enumerate security requirements
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
  - Auditability
  - Access control
  - Privacy
  - …

Secrecy, Confidentiality, Privacy, Anonymity

- Often considered synonymous, but are slightly different
- Secrecy
  - Keep data hidden
  - E.g., Alice kept the incriminating information secret
- Confidentiality
  - Keep (someone else's) data hidden from unauthorized entities
  - E.g., banks keep much account information confidential
- Privacy
  - Keep data about a person secret
  - E.g., to protect Alice's privacy, company XYZ did not disclose any personal information
- Anonymity
  - Keep identity of a protocol participant secret
  - E.g., to hide her identity from the web server, Alice uses The Onion Router (TOR) to communicate

Integrity, Authenticity, Authentication

- Sometimes used interchangeably, but different
- Data integrity
  - Ensure data is “correct” (i.e., correct syntax & unchanged)
  - Prevents unauthorized or improper changes
  - E.g., Trent always verifies the integrity of his database after restoring a backup, to ensure that no incorrect records exist
- Entity authentication or identification
  - Verify the identity of another protocol participant
  - E.g., Alice authenticates Bob each time they establish a secure connection
- Data authentication
  - Ensure that data originates from claimed sender
  - E.g., For every message Bob sends, Alice authenticates it to ensure that it originates from Bob

Temporal Properties

- Age
  - Prove that data exists before a certain time
  - Lower bound on the duration of existence
- Freshness
  - Prove that data was created after an event
  - Upper bound on the duration of existence
- Temporal order
  - Verify ordering of a sequence of events

Other Properties

- Auditability
  - Enable forensic activities after intrusions
  - Prevent attacker from erasing or altering logging information
- Availability
  - Provide access to resource despite attacks
  - Denial-of-Service (DoS) attacks attempt to prevent availability

4. Approaches to Achieve Security

- No security
  - Legal protection (deterrence)
  - Innovative: patent attack, get protection through patent law
- Build strong security defense
  - Use cryptographic mechanisms
  - Perimeter defense (firewall), VPN
- Resilience to attack
  - Multiple redundant systems (“hot spares”)
- Detection and recovery (& offense ?)
  - Intrusion detection system
  - Redundancy, backups, etc.
  - Counterstrike? (Legal issues?)

Threat Models

- Can’t protect against everything
  - Too expensive
  - Too inconvenient
  - Not worth the effort
- Identify most likely ways system will be attacked
  - Identify likely attackers and their resources
    - Dumpster diving or rogue nation?
  - Identify consequences of possible attacks
    - Mild embarrassment or bankruptcy?
  - Design security measures accordingly
    - Accept that they will not defend against all attacks

Think Like an Attacker

- Adversary is targeting *assets*, not defenses
- Will try to exploit the *weakest* part of the defenses
  - E.g., bribe human operator, social engineering, steal (physically) server with data

Takeaways

- Security: important but difficult
- Security is not absolute
  - Attacker
  - Properties
  - Cost
- Security is about managing risk in the presence of an adversary