SECRETS

Bay St. Hacked

-Potash deal

-7 law firms targetted

-Documents likely stolen according to consultants but firms won't admit it

State Espionage

-China to blame?

-Attacks in the US led by secret Chinese military unit according to Mandiant, security consultancy

Shhh...

-No details, but the attacks for secrets are the same as for money, whatever the motive

MONEY

2011 Six Figure Loss

-Toronto firm lost "six figures"

-Bookkeeper's computer hacked

-By "Trojan Banker Virus"

-Stole money from firm's online bank account

2013 US Firm Hacked

-US firm lost $336k

-Keyboard logging software used to steal wire transfer information + wire $

-Bank and law firm in litigation over who should have to pay

-Similar situation bankrupted an escrow service in 2013, thieves stole $1.6 million

Wire Transfers and ACH Transfers

-The two targets are online banking/wire transfer facilities and payroll systems

-Payroll systems are targetted by hacking in and adding new fake employees who then receive money through ACH transfers (same way you get paid by your firm)

2013 Title Company Hacked

-Lost $1.7 million through a combination of wire transfers and ACH

Bitcoin Ransomware

-Encrypts your hard drive and then you have to pay to unlock it

-If you don't pay, you lose all the files on the computer

-What's interesting is that this is a new money method b/c uses Bitcoin, a digital currency that is anonymous and easy to transfer

HOW

Spear Phishing + Website Exploits

-Two main methods

Spear Phishing

-Likely how the Toronto firm's bookkeeper lost "six figures"

-Hackers send an email specially crafted for the recipient (who they've identified as someone with access to money), e.g. "Confidential: 2014 Partner Salaries"

-Email has virus in it, infects computer

-In the bookkeeper case the virus created a fake bank site and it had a fake phone number that connected the bookkeeper with a fake customer service rep who assisted in the theft

Website Exploits

-Very common method of attack

Target

-Likely method of attack against Target that's in the news

-110 million customers ultimately affected

How They Did It

-Website exploit

-Take over one server and use it to gain access to more

-Found the servers that had the software for the card machines

-Changed the software on the card machines to steal information

-Stole card info + personal information

Class Actions

-70 filed so far

You Don't Have Better Security Than Target

-Your security isn't better than Target so this is a problem for you

-You should take security seriously, it may cost you money and your reputation

Other Sites Can Expose You

-If other sites are leaking your passwords then thieves may gain access that way

-There's a provincial law insurer that stores passwords in plaintext that if stolen could grant access to many services

-Security includes the sites you use

Thieves Probably Have Access To Your Files

-I've posted a series of security tips that address the dangers raised in this presentaiton