Lessons from the recent hack attacks

Ramki

Jun 11

No. of high profile breaches of late..

- IMF
- Citi bank
- White house
- BofA
- Michaels
- SONY

No. of high profile breaches of late..

- Epsilon
- Comodo
- Heartland
- T.J.Maxx
- RSA
- PayPal
- Google
- Lockheed
- AT&T etc

And probably the biggest..

- Luiz security claimed they had hacked the CIA!
- The same group of hackers has claimed responsibility for recent attacks on websites operated by
  - the U.S. Senate,
  - Sony Corporation,
  - Nintendo and the
  - Public Broadcasting System television network in the United States.

Attacks are becoming..

- **More frequent**
- **More brazen**
- **More innovative (use of camouflage like a DDOS attack at the same time when infiltration happens)**
- **More sophisticated (like using stolen secure id data)**
- **More focused (which weakness to target)**
- **More international (FBI now works with many countries)**
- **More widespread (even after arrest of Albert Gonzalez, the mastermind behind the TJX and Heartland breaches, there is no reduction)**
- **MORE HIGH PROFILE**

Verizon breach report – Apr 11

- Hacking, at 50 percent, and malware, at 49 percent, are the most prominent types of attack, with many incidents involving weak or stolen credentials and passwords;
- Physical attacks, such as **skimming** at ATMs, **pay-at-the-pump** gas terminals and POS systems, for the first time rank among the three most common ways to steal information, comprising 29 percent of all investigated cases;
- Outsiders are responsible for 92 percent of breaches, while the percentage of insider attacks dropped from 49 percent in 2009 to 16 percent in 2010.

Verizon report contd.

- 86 percent of the year's breaches were discovered by third parties;
- 97 percent were avoidable through simple or intermediate controls;
- 89 percent of the corporate or organizational victims were not compliant with the **Payment Card Industry Data Security Standard** at the time of the hack.

Reasons..

- Thieves share information in online forums like Xakep.ru, HackZone.ru
- There are tens of thousands of hackers sharing the info./knowledge
- Price for credit card info. Is increasing
- Some hackers specialize in prying out customer names, account numbers and other confidential information and sell it in internet bazaar
- Some hacking team members do not know each other!
- Use info. Gained in one hack for another –e.g data gained in RSA was used to break into Lockheed Martin Corp., US's largest Defense contractor and L-3

Reasons contd.

- Certain countries specialize in this: Eastern Europe, including Russia, Belarus, Ukraine and Romania
- With every capture/ take down , they regroup!
- In most companies every step along the payment chain is outsourced from the time a card is swiped to the time a monthly statement arrives, leaving plenty of openings for enterprising thieves.
- Security is hampered by a patchwork of data protection laws and regulatory agencies, each with limited mandates.
- Credit card lenders are in the business of reducing the financial losses stemming from fraud, not preventing data theft in the first place.

Reasons contd.

- Banks have no incentive to control this as they charge heavy charge back fees on the merchants and also recover cost of fraudulent purchase from them.
- Encrypting data as it flows across the entire payment network would make data far less vulnerable to being extracted by thieves but this is not done in many cases.
- Repetitive attacks using various vulnerabilities
- Reason for attack could be as simple as ‘we do not like you’; ‘we hate you as a nation’ etc

Reasons contd.

- A security expert commenting on Michaels breach said:
  - "It is definitely a highly targeted effort by organized crime, who did their homework, identified vulnerable hardware; and swooped in, in a coordinated effort to maximize their window of opportunity; also it was audacious when you consider that equipment needed to be physically tampered with, which is certainly a bit higher risk than a remote breach attempt."
  - Probably a forerunner for more such co-ordinated attacks

Reasons contd.

- Spear phishing, a rapidly proliferating form of fraud comes with a familiar face:
  - messages that seem to be from co-workers, friends or family members, customized to trick you into letting your guard down online.

- Examples:
  - an e-mail from your mother saying she needs your Social Security number for the will she's doing.
  - e-mail sent to the head of a company that appears to be from the Inland Revenue Service
  - A fake but convincing Gmail login screen used by attackers to dupe targets into submitting their passwords
  - e-mail from what appeared to be employer's human resources department that asked for personal information to make a payment or saying "your bonus" or "your incentive"

Reasons contd.

- FBI states Vishing attacks are increasing
  - Vishing starts with an e-mail, like phishing, but requests that end-users contact a particular institution by phone in order to resolve an issue or re-secure personal data.
- Companies are not updating their software/ patches fast enough

Citi bank

- Compromised/ stolen:
  - Names, account numbers, e-mail addresses and transaction histories of more than 200,000 or more Citi customers. (Previous breach in 2009)
- How?
  - By using customer Web site as a gateway to bypass traditional safeguards and impersonate actual credit card holders..
  - Once inside, hackers leapfrogged between the accounts of different Citi customers by inserting various account numbers into a string of text located in the browser's address bar.
  - The hackers' code systems automatically repeated this exercise tens of thousands of times allowing them to capture the confidential private data.
- Action: Contacting customers whose data was stolen

IMF

- Compromised:
  - Possibly confidential information about numerous countries in financial trouble. Some of the agreements with troubled countries like Greece can be ‘political dynamite’.
- How?
  - New kind of malware, one that gave hackers broad access and views of IMF's systems
  - First entry gained thru targeted **spear phishing** attack that compromised someone internally
  - related to a sophisticated digital break-in at RSA Security that took place in March 11
- Action:
  - World bank immediately severed its link with IMF website

White house

- Compromised:
  - Personal G mail accounts of many white house staffers (many departments), human right activists, journalists and South Korea's government.
  - Google says this was a Chinese Government job which they deny!
- How?
  - Targeted e-mails that appeared to be tailored to their victims.
  - Recipients were asked to click on a link to a phony Gmail login page that gave the hackers access to their personal accounts!

Sony

- Compromised:
  - Personal data relating to 52000 Play station game customers.
  - This attack followed a devastating security breach of Sony's PlayStation Network, which forced it offline in late April for more than a month after personal data including credit card details of tens of million user accounts were stolen.
- How?
  - A hacker group calling itself LulzSec used a "simple" attack on a "primitive" security hole that gave it full access to the Sony Pictures internal database
  - Distributed denial of service attacks (DDOS) crippling its PlayStation gaming network and Qriocity music service last month camouflaged simultaneous intrusions that resulted in the exposure of personal identifiable information
  - Forensics expertise from at least three firms was needed to pinpoint exactly what happened!

Bank of America-Big and scary

- Compromised:
  - names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, e-mail addresses, family names, PINs and account balances of 300 plus customers
  - **more than $10 million was drained from customer accounts.**
- **How?**
  - **Security breach –internal or external**

Michaels

- Compromised:
  - Breach affecting stores in 20 states which led to fraudulent purchases and later ATM withdrawals from banks
- How?
  - Fraudsters replaced legitimate point-of-sale PIN pads with tampered ones.
  - "[Fraudsters] get around EMV chip by disabling the part of the POS device that reads the chip, so, then the customer is forced to swipe the mag stripe to make the transaction."
- Action taken:
  - Michaels removed some 7,200 PIN pads from most of its 964 U.S. stores and
  - Some institutions with customers and members affected by the Michaels breach took proactive action, such as freezing accounts and posting notices on their websites.

Comodo – too big to fail

- Compromised:
  - Web sites rely on third-party organizations, like Comodo, to provide “certificates” that guarantee sites’ authenticity to Web browsers i.e whether ’https’ is reliable.
  - The Hacker automatically created certificates for Web sites operated by Google, Yahoo, Microsoft, Skype and Mozilla. With the certificates, the hacker could set up servers that appear to work for those sites and try to view the unscrambled e-mail of millions of people
- How?
  - A talkative and professed patriotic Iranian hacker infiltrated an Italian computer reseller and used its access to Comodo’s systems to automatically create certificates.

T.J.Maxx

- Compromised:
  - A hacker stole data from at least 45.7 million credit and debit cards of shoppers at off-price retailers including T.J. Maxx and Marshalls
- How?
  - Hackers “had access to the decryption tool for the encryption software utilized by TJX.”

RSA

- Compromised:
  - information being extracted from the company's IT systems.
  - Security token information breached.
- How?
  - extremely sophisticated attack aimed at its SecurID two-factor **authentication** products.
  - It is an APT (Advanced persistent threat) which refers to sophisticated and clandestine means to gain continual, persistent intelligence on a group such as a nation or corporation.
- Action taken:
  - New security tokens issued for sensitive operations.

Prevention

- Against Phishing:
  - layered fraud-prevention approach that starts with secure browsing and includes multiple layers of user and account monitoring, and appropriate interventions.
- Law:
  - Pentagon to consider cyber attacks as acts of war!
- Monitoring:
  - Strong transaction monitoring and behavioral analytics
- Third party vendors:
  - Ensuring Third parties with which companies work rely on the same high-level security measures as they do.

Prevention contd.

- User education- US-cert:
  - Do not follow unsolicited links or attachments in e-mail;
  - Use caution when providing personal information online;
  - Verify the legitimacy of e-mail by contacting the sender directly;
  - Review common best practices for **avoiding e-mail scams** and **socially engineered attacks**.

Prevention contd.

- Josh Corman research director of Enterprise security practice at The 451 group has 4 recommendations:
  - 1. Limit access
  - 2. Pile on layers of security and get up-to-date (Many attacks were exploiting easy techniques like default passwords or out of date Apache or Web-servers)
  - 3. Include breach response in DRPs
  - 4. Admit fault and negotiate

Prevention in the future..

- **'Digital ants' seek viruses to protect computer networks.**
  - "The idea is to deploy thousands of different types of digital ants, each looking for evidence of a threat;
  - As they move about the network, they leave digital trails modeled after the scent trails ants in nature use to guide other ants.
  - Each time a digital ant identifies some evidence, it is programmed to leave behind a stronger scent
  - Stronger scent trails attract more ants, producing the swarm that marks a potential computer infection."
    - **Errin Fulp, a professor of computer science at Wake Forest University working on this**

References

- Thieves Found Citigroup Site an Easy Entry - NYTimes.com
- IMF Attack: 1 of Dozens of Breaches? Bankinfosecurity
- Sophisticated Cyberattack Is Reported by the I.M.F. - NYTimes.com
- Citi Breach Exposes Card Data- Bankinfosecurity
- Citi Data Theft Points Up a Nagging Problem - NYTimes.com
- Spear Phishing Uses Friendly Faces to Spread E-Mail Fraud - NYTimes.com

References contd.

- Gmail Hacking of White House Affected Diverse Departments - NYTimes.com
- Hacker Group Claims Responsibility for New Sony Break-In - NYTimes.com
- Pentagon to Consider Cyberattacks Acts of War - NYTimes.com
- Researchers working on ‘digital ants’ to flush out virus in computer networks ibtimes.com
- Michaels Breach Bigger than Reported Bankinfosecurity
- Michaels Breach Patterns Showed Fraud Bankinfosecurity

References contd.

- An Attack Sheds Light on Internet Security Holes. NY times
- T.J. Maxx theft believed largest hack ever. Msnbc.com
- Phishing Scheme Targets PayPal, BofA bankinfosecurity
- Hackers Target RSA's SecurID Products Bankinfosecurity
- FBI warns that vishing attacks are on the rise- Arts technica

References contd.

- Sony: DDoS Masked Data Exfiltration Bankinfosecurity
- Verizon Breach Report Incidents Are Up Bankinfosecurity
- Epsilon Breach: Risks and Lessons Bankinfosecurity
- Epsilon Breach: How to Respond Bankinfosecurity
- 'Digital ants' seek viruses to protect computer networks. Physorg.com
- Hackers-Claim-Breach-of-CIA-Website. VOA
- Breach Avoidance: 4 Tips Bankinfosecurity