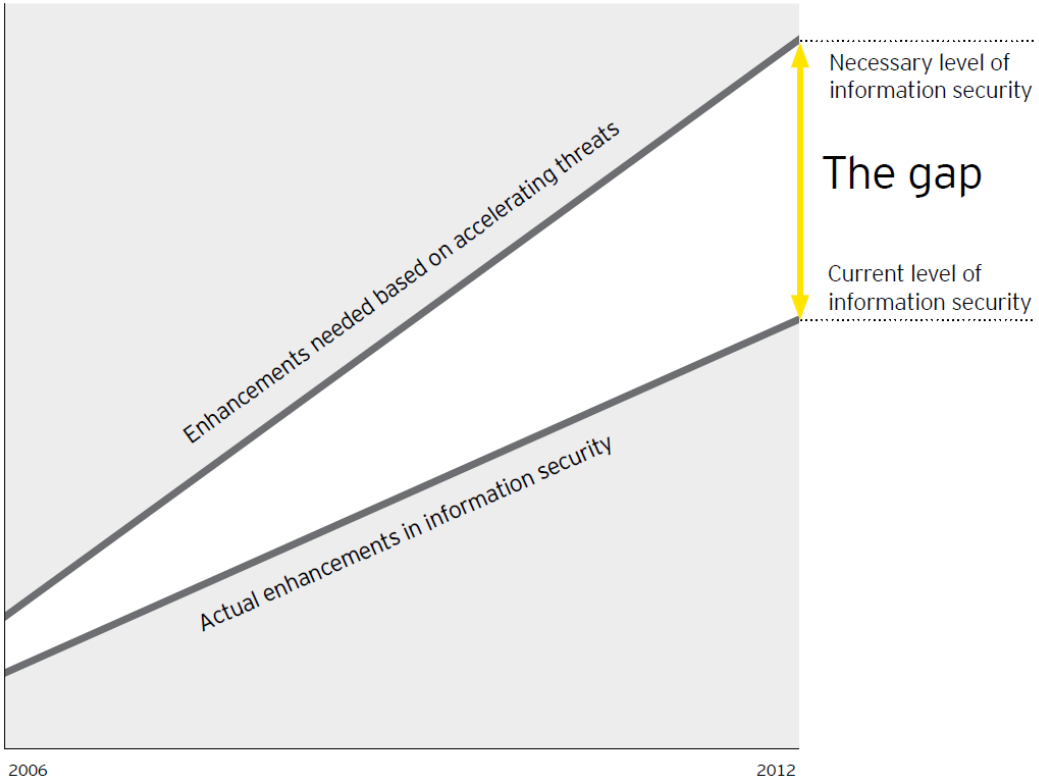
Cyber Security Trends

Ernst & Young

Quality In Everything We Do

Emerging trends and threats for 2013

- Unauthorized access to corporate data through compromised mobile devices
- Theft of personal information via social media
- Ransomware
- Hactivism
- Advanced persistent attacks
- Spear phishing attacks



Cyber threats: a few statistics

- 1 in every 284 emails contains malware (Government of Canada)
- 45% of malware infections in 2011 required user involvement (Microsoft report)
- Every 3 seconds, an identity is stolen on-line (Symantec report)
- Over 120 countries now use the Internet for cyber-espionage operations (McAfee)

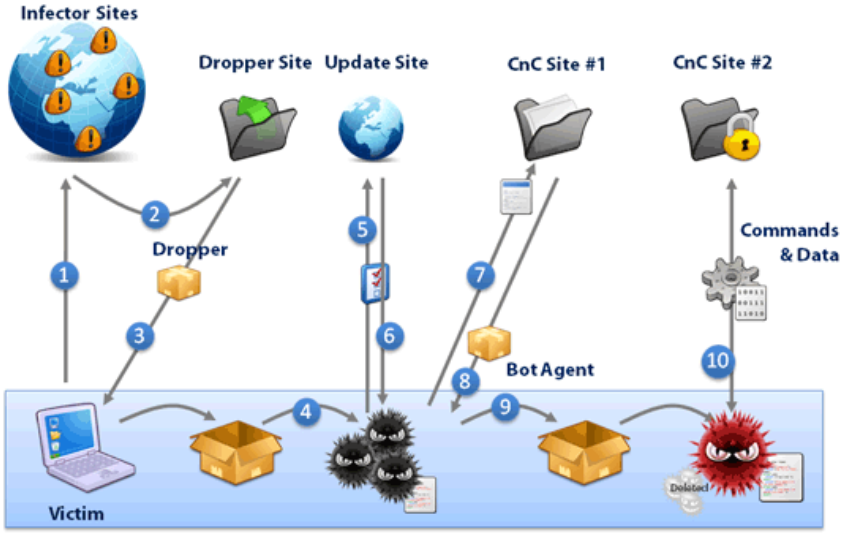
- 80 major US law firms were victims of cyber attacks in 2011 (American Bar Association)
- 88% of Fortune 500 companies are infected with advanced viruses remotely controlled by hackers, also known as botnets (RSA report)

Advanced cyber attacks

- Who is behind these attacks?
  - Well-resourced, highly capable and relentless class of hackers
  - Some are sponsored by foreign states and criminal networks
  - Some of them will sell their services to the highest bidder (Malware As A Service)
- What motivates them?
  - **Money:** access to people's identity credentials to commit fraud or extortion
  - **Competitive advantage:** access to intellectual property
  - **Cyber warfare:** control of a country's critical infrastructures
- How do they get in?
  - Targeted phishing attacks
  - Zero-day virus (a new virus not detectable by conventional anti-virus)
  - Password cracking
  - Weaknesses in web portals

How do they get in?

Here is an example:



1. An ATP entices a user to access an infector website through “spear phishing”
2. Once this is done, the link is transferred to a “dropper site”
3. A “zero-day” virus is downloaded on the user’s computer, undetected by firewalls
4. Once on the user’s computer, the zero-day virus installs itself, undetected by anti-virus software
5. Once installed, the virus calls its master for instructions
6. Instructions are received to scan the computer to obtain details on the environment (operating systems, missing patches, user privilege, etc.)
7. The information collected is uploaded to a command and control site
8. With this information, a more powerful virus or Trojan can be custom made to exploit the vulnerabilities identified on the computers
9. Once downloaded and installed on the computers, this zero-day malware can be programmed to do all sorts of nefarious things, including capturing user passwords, scanning the network and replicating itself on other computers
10. When it reports back to a command and control site (a different one each time), the information sent is usually encrypted to ensure that it remains unnoticed by Data Loss Prevention systems or security monitoring tools

Traditional safeguards

- **They don’t work against advanced cyberattacks**
- **Firewalls:** attacks are embedded within generic http Web traffic
- **Intrusion Prevention System (IPS):** Signatures, packet inspection, DNS analysis and heuristics will not detect anything unusual in a zero-day malware, especially if the code is heavily disguised or delivered in stages
- **Antivirus & Web malware filtering:** Since the malware and the vulnerability it exploits are unknown (zero-day), and the Website has a clean reputation, traditional antivirus and Web filters will let it pass
- **Email spam filtering:** Spoofed phishing sites use dynamic domains and URLs, so blacklisting lags behind criminal activities. It takes more than two days to shut down the average phishing site.

Who is targeted? Governments

CBCnews | Politics

Foreign hackers attack Canadian government

Computer systems at 3 key departments penetrated

By Greg Weston, CBC News Posted: Feb 16, 2011

An unprecedented cyberattack on the Canadian government also targeted Defence Research and Development Canada, making it the third key department compromised by hackers, CBC News has learned.

The attack, apparently from China, also gave foreign hackers access to highly classified federal information and also forced the Finance Department and Treasury Board — the federal government's two main economic nerve centres — off the internet.

Defence Research and Development Canada works to assist in the scientific and technological needs of the Canadian Forces. It is a civilian agency of the Department of National Defence.

The cyberattack, first detected in early January, left Canadian counter-espionage agents scrambling to determine how much sensitive government information may have been stolen and by whom.

Who is targeted? Financial institutions

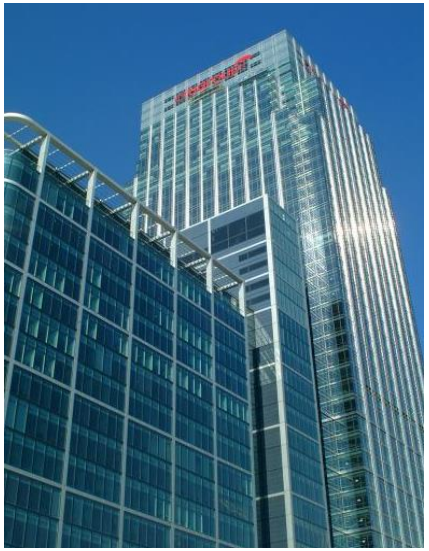
BGR

Citigroup hacked, 200,000 accounts compromised

By: Todd Haselton | Jun 10th, 2011 at 02:30AM

On Thursday Citigroup announced that hackers had breached its systems in May and accessed personal data from 200,000 accounts — about 1% of its customers.

The hackers managed to steal customer email addresses, contact information and account numbers, but Reuters reported that other information such as birth dates, Social Security Numbers and credit card expiration dates were not accessed. “We are contacting customers whose information was impacted. Citi has implemented enhanced procedures to prevent a recurrence of this type of event,” Citigroup spokesperson Sean Kevelighan, said. “For the security of these customers, we are not disclosing further details.” It is currently unclear who was responsible for the breach.



Who is targeted? Utilities

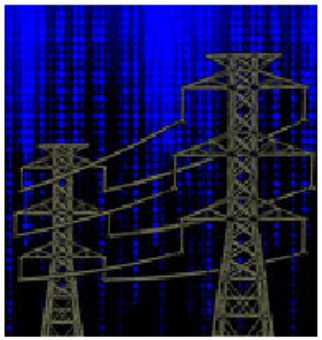
Bloomberg

Power-Grid Cyber Attack Seen Leaving Millions in Dark for Months

By Brian Wingfield - Feb 1, 2012

A blackout that swept parts of North America in August 2003, leaving 50 million people in the dark for as long as four days, provides a glimpse of the havoc a cyber attack could inflict on the nation's power grid.

Internet-based terrorists would be capable of causing blackouts "on the order of nine to 18 months" by disabling critical systems such as transformers, said Joe Weiss, managing director of Applied Control Solutions LLC, a Cupertino, California-based security consulting company.



"The dollars are incalculable," Weiss said in a phone interview. The 2003 event, triggered when a power line touched tree branches in Ohio, caused losses of as much as $10 billion, according to a study by the U.S. and Canadian governments.

Energy companies including utilities would have to increase their investment in computer security more than seven-fold to reach an ideal level of protection, according to a survey done for Bloomberg Government by the Ponemon Institute LLC, a data- security research firm based in Traverse City, Michigan.

Who is targeted? High-tech firms

REUTERS

Hackers breached U.S. defense contractors

(Reuters) - Unknown hackers have broken into the security networks of Lockheed Martin Corp (LMT.N) and several other U.S. military contractors, a source with direct knowledge of the attacks told Reuters.

They breached security systems designed to keep out intruders by creating duplicates to "SecurID" electronic keys from EMC Corp's (EMC.N) RSA security division, said the person who was not authorized to publicly discuss the matter.

Who is targeted? Law firms

Bloomberg

China-Based Hackers Target Law Firms to Get Secret Deal Data

China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant zeroed in on offices on Toronto's Bay Street, home of the Canadian law firms handling the deal.

Over a few months beginning in September 2010, the hackers rifled one secure computer network after the next, eventually hitting seven different law firms as well as Canada's Finance Ministry and the Treasury Board, according to Daniel Tobok, president of Toronto-based Digital Wyzdom. His cyber security company was hired by the law firms to assist in the probe.

Who is targeted? On-line retail industry

SecureWorks

Hacker Attacks Targeting Retailers Up 43%

Dell SecureWorks®, a leading provider of information security services, reported that hacker attacks targeting its retail customers increased 43 percent between the last nine months of 2010 and the first nine months of 2011. From January through September 2011, Dell SecureWorks blocked an average of 91,500 attacks per retail customer, as compared to 63,581 attacks per retail customer April through December 2010.

"Based on the attacks we detected in the first nine months of this year, criminals are more aggressively using the web as a primary attack vector for both clients and servers," said Jon Ramsey, Dell SecureWorks CTO. "We saw a significant increase in SQL Injection attacks against servers and exploit packs hosted on web sites, which contributed to the overall rise in retail attacks."

How to protect against advanced attacks?

- **Traditional protection mechanisms don't work:**
  - Firewalls: APT embed their attacks within generic http Web traffic
  - Intrusion Prevention System (IPS): Signatures, packet inspection, DNS analysis and heuristics will not detect anything unusual in a zero-day malware, especially if the code is heavily disguised or delivered in stages
  - Antivirus & Web malware filtering: Since the malware and the vulnerability it exploits are unknown (zero-day), and the Website has a clean reputation, traditional antivirus and Web filters will let it pass
  - Email spam filtering: Spoofed phishing sites use dynamic domains and URLs, so blacklisting lags behind criminal activities. It takes more than two days to shut down the average phishing site.
- **The solution: a multi-layer cyber protection program**

How to reduce exposure to cyber attacks?

- Create cyber intelligence team to deploy proactive security measures
- Implement multiple security layers
  - Upstream protection by your telecom carrier (1st layer)
  - Protection at the network perimeter with advanced cyber security tools (2nd layer)
  - Advanced protection on your computer devices (3rd layer)
- Test your resilience to cyber attacks
  - Test your infrastructure (e.g., penetration tests)
  - Test your processes (e.g., table-top simulation exercises)
  - Test your people (e.g., social engineering, phishing, etc.)
- Produce security metrics that make business sense
  - Impact on operations
  - Impact on finances
  - Impact on reputation
  - Impact on compliance requirements
- Increase the level of awareness at all levels

QUESTIONS

Ernst & Young

Quality In Everything We Do