Enabling Cyber Security Resiliency at the Ottawa Police Service

Daniel Steeves
Chief Information Officer
Ottawa Police Services
steevesd@ottawapolice.ca
Distributed Denial of Service

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
The Attack!!

- **Timing**
  - Wed, Nov 19^{th}
    - Communications were threatened by DDOS coming
  - Fri, Nov 21^{st}
    - Hacker call goes out
- **Multi-Pronged**
  - Website [social engineering]
  - E-mail Pipe
  - Firewall
The Targets

- Ottawa Police
- Guelph Hydro
- Ottawa(.ca)
- City of Waterloo
- Telus.com/.ca
- WindMobile.ca
- koodomobile.com
- fido.ca
- Supreme Court of Canada
The Impact

• The OPS Experience
  – ISP shuts down website host line due to attack volume
  – Millions of hits on the Firewall in a 2 hr timeframe

• The Other Targets
  – City Website hacked briefly
  – Supreme Court targeted

• The Community Perception
  – Media coverage
The Response

• Call to IBM Exec Team
  – Sun afternoon
  – Mon morning – team stood up
  – The importance of critical partners
• Creating the Solution
  – Eliminating the target vectors [website/email/firewall]
  – Physical migration of the website
  – Installing a shield: 30 hrs
  – Triangulation and Monitoring
The Solution

Akamai Product Sequencing:

• Web Application Firewall
  – to deny application layer and volumetric attacks (e.g. SQL Injection, Cross Site Scripting, DDoS, etc.)

• FastDNS
  – set as primary DNS infrastructure to protect OPS’ DNS from volumetric attacks that would deny service to users trying to access the site

• SiteShield
  – to deny attackers direct access to the web infrastructure
The Solution [con’t]

• IBM Security Operations Centre
  – to ensure that attacks can be monitored and dealt with 24x7 in real time
• Proof Point
  – E-mail monitoring off your doorstep
• SoftLayer Infrastructure-as-a-Service (IaaS)
  – SoftLayer’s cloud service provides server hosting, firewall, network and storage, in an Ontario data centre through a simple self-service portal … fast and flexible!
The Results

• Some Stats
  – Website stood up Nov 28\textsuperscript{th} [7 days later]
  – Akamai DNS services served 192,629 requests Nov 28\textsuperscript{th} - Dec 1\textsuperscript{st}
    • Sustained 2 hr attacks became 2 min probes
    • 90\% of all website hits handled at the edge, not at OPS infrastructure
    • Denied malicious probes such as:
      – Remote File Inclusion
      – ShellShock exploit attempts
      – Rogue Web Site Crawlers and scanners
Lessons Learned

• Social Engineering Techniques
  – Spoofing legitimate police staff
  – Phone / E-Mail

• Agility
  – Time to Solution

• Cyber Security is Strategic
  – Avoid tactical reactions
One of The Hackers

August 10th 2015
Aerith@TWITRis4tards

– aha, just read the CIO of Ottawa Police article - what you didn't like the fake ID I made Dan Malloy?
– Don't think you're special Ottawa, I did it to Toronto also and for 3 hours had their MX server redirecting to mine.
When a Hacker gets Hacked

August 20th 2015 - Aerith@TWITRis4tards becomes Aerith@QUVREijAN5e0DML

• @Justin_Ling it's funny, because I stole this new account also
• @Justin_Ling lol, well my account was super easy to hijack, it used a temp disposable email of retard@mailinator.com
• I'm just hoping you used a residential IP or your opsec isn't up to par, so I can watch a swat descend upon your house.
• It's amusing…I hacked it from the original owner anyway
• @CTVMercedes new twitter since @twitris4tards was "haxxed" by some skid who figured out I used a disposable email
Future Considerations

• Attacks will continue
• www = Wild Wild West
• Public Safety really needs to catch up
• The Question?
  – What should police services and similar corporate entities be doing to secure their environments?
IBM Security - Intelligence, Integration and Expertise

Dave Millar
Security Solutions Executive
IBM Canada
dmillar@ca.ibm.com
Silver Bullet?

There is no ‘Silver bullet’ to protect yourselves from malicious cyber-threats that include Hacktivists, Nation states, Insiders, etc.
It’s more like This.....
How do I know what to do?

or really . . .

What do I do first?
Assess

You need to know where you are to know where you are going.

Assess your current threat posture
- Perform a threat/risk assessment
- Where are you today?
- Where do you need to be?
- What are the gaps?
- What is the plan?
Protect

Protect yourselves from Basic and Advanced Threats

PREVENT BASIC THREATS
- Viruses
- ‘known’ malware
- Distributed Denial of Service
- SQL injections
- Patchable Vulnerabilities
- Spear-phishing

DETECT ADVANCED THREATS
- ‘Zero-Day’ Malware
- Malicious Insider activity
- Non-malicious Insider activity
- Anomalous behaviour
- Non-patchable Vulnerabilities
Respond

Respond to **REAL** threats with a integrated plan

- Have someone performing 24/7 threat monitoring who is watching the infrastructure for Indicators of Compromise
- Have an incident response plan documented that is rehearsed
- Have a contract with a company who can provide assistance, guidance, and forensic support
Manage

Manage the security program by Operationalizing the security technology, processes and people

**Managed Services**
- Hosted and cloud-based security services deliver the highest level of security intelligence
- Managing your security operations through integrated tools, strategies, intelligence, analytics and staff skills
Seek External Help!

To help you effectively establish your security operations

1. Security threat monitoring
   Around the clock visibility, analysis and reporting of billions of log events from Intrusion Prevention Systems (IPS), firewalls and routers across multiple devices

2. Security incident management
   Define, prioritize and manage incidents based on corporate policy, business controls and regulatory requirements

3. Personnel recruitment, retention and management
   Network support desktop support, troubleshooting, script writing, ongoing training and auditing

4. Process development and optimization
   Document and implement analytical, business, operational, technology processes and procedures

5. Emerging threat strategy
   Threat service subscriptions and security metrics
USA National Level View

U.S. Victims of Chinese Cyber Espionage over the past five years

Ref: Bill Bonner’s Diary
Internet of Things – Baby Monitors

Affected devices

- Gyonii (GCW-1010)
- iBaby (M3S)
- iBaby (M6)
- Lens (LL-BC01W)
- Philips (B120/37)
- Summer (28630)
- TRENDSnet (TV-IP743SIC)
- WiFiBaby (WFB2015)
- Withing (WBP01)

Ref: Zack Whittaker for Zero Day
3D Printed Wu Ying Shoes [Shadowless]

The latest weapon in enterprise hack attacks

Ref: Charlie Osborne for Zero Day
3D Wu Ying Shoes – SexyCyborg

Ref: Charlie Osborne for Zero Day
Corporate Implications

Aug 2015 a US federal court ruled – the Federal Trade Commission (FTC) now has the power to go after corporations that fail to take adequate measures to protect customer information from hackers.

Because

- **Wyndham** had major data breaches in 2008 and 2009.
- Hackers stole credit card numbers and other personal information from 619,000 customers.
- This resulted in more than $10.6 million worth of fraudulent charges. Now the FTC wants to make sure Wyndham pays for its lack of preparedness.

Ref: Investment U Plus
Corporate Implications

The FTC is also considering a case against Target over the hack that exposed data for as many as 40 million customers. Some US based stats:

• A whopping 91% of U.S. companies have been targeted by a cyber threat within the past year.
• There were 118,000 attempted attacks PER DAY in 2014.
• Successful hacks on Anthem, JPMorgan and Sony show no industry or company is truly safe.
• Last year, each successful cyber attack in the U.S. cost the affected company an average of $12 million.
• The amount of damages per incident has doubled in the past five years.

Ref: Investment U Plus
Corporate Implications

The corporate question now becomes –

*Will we spend money on cybersecurity measures or huge court settlements?*
Questions?

Daniel Steeves
CIO
steevesd@ottawapolice.ca