Anatomy of a Cyber Attack

(The information herein has been previously reported and published in various forms in the public domain)

Rich McClain
Director, Information Technology
Hunton & Williams LLP
Anatomy of a Cyber Attack

- **Code Name:** Caspian
- **Timeframe:** December 2010 – February 2011
- **Key Players:**
  - “Big Bank”
  - Hunton & Williams
  - WikiLeaks/Julian Assange
  - Anonymous/Anon
  - IRCs (Internet Relay Chat Rooms)
  - Global Consulting and Security Firm
  - “Big Data” eDiscovery Software Firm
  - Global Security Operations Center
  - Law Firm Software, Hosting, and Intelligence Provider

- **Other:**
  - Boutique Security Firm (wanna-be protagonists)

- **Nature of Attack:**
  - Began as an engagement to help a client mitigate liability and reduce damages from a purported, but unconfirmed, data breach
  - Became a targeted cyber-attack on the organizations and individuals involved when it appeared that counter-measures were being considered (by wanna-be protagonists) to not only thwart but also impair the attacker.
Phase 1  – “A Typical Day at the Office”

• WikiLeaks announces they are going to publish a trove of Big Bank confidential information
• Big Bank engages Hunton & Williams to help research possible data breach, and manage/mitigate liabilities
• Structured engagement team forms - legal, technical, bank experts
• Team has meetings, documents the situation/recommendations, send lots of emails
Phase 2 – “The Mosh Pit”

• Key Players focused on core mission establishing plans, information, personal relationships, etc
• Boutique Security Firm tries to join the party and “help”
  – Lots of ideas, superfluous information
  – Devise a plan to supposedly destroy WikiLeaks
  – Propose plan to various Key Players with no success
  – Decide to tout plan in the international press
Phase 3 – “The Attack Begins”

• WikiLeaks and Anonymous hear about plan, and decide they need a copy
• Within 24 hours, Anonymous breaches Boutique Security Firm, steals the plan, along with thousands of emails and a Facebook site
• Other Players implicated in the emails, albeit unfounded, now become targets
• Anonymous starts a counter-insurgency
• IRC Rooms start to buzz
Phase 4 – “Legitimate Paranoia Sets-in”

• Are Hunton & Williams partners being virtually and physically stalked?
• Should we remove all email and documents from our systems?
• Do we have insider sympathizers/threats?
• Are the Global Consultants really “white hats”?
• Was the QAKbot malware event in November a preliminary staging attack?
• Will I be fired for being a week late in applying this month’s security patches?
Phase 5 – “Cooler Heads Manage Chaos”

• Priorities are established based on judgment and facts
• Task assignments made
• Details really matter
• Additional technical and institutional safeguards implemented in record time
• Substantial human capital & intelligence applied to monitor the threat
Phase 6 – “Tenacity & Discipline Prevail”

• Relatively strong defenses combined with careful monitoring is key
• The attackers’ thrill with the mission apparently subsides after countless hours…days…weeks
• Other events/targets become interesting and gain attention
Phase 7 – “Cleanup & Lessons Learned”

• “The Basics” – strong and diverse passwords; updated firewalls and patches; due-care in email
• Employ best practices for communicating and storing data before, during and after an attack
• Build strong relationships between legal and technical professionals
• Establish relationships with qualified and ethical players
• Recognize that no organization is immune or “impeccable”
And just when you thought it was over.....

Anonymous leaks big bank secrets in spy revenge hack

Hacktivists enraged by suggestion financial giant snooped on them

27th February 2013

Miscreants affiliated with hacking collective Anonymous have dumped online a huge cache of data supposedly lifted from insecure systems at a big bank contractor.

The self-styled Anonymous Intelligence Agency (Par:AnoIA) leaked 320MB of emails and other information that suggests the banking giant is running an online intelligence gathering operation against hacktivists.
The Privacy Team at Hunton & Williams

• More than 25 privacy professionals in the US, EU and Asia
• Our privacy clients include 6 of the Fortune 10 companies
• Lisa Sotto heads the firm’s Global Privacy and Cybersecurity practice
• Top-ranked privacy practice, including ranked in “Band 1” for Privacy and Data Security in Chambers Global, Chambers USA and Chambers UK
• Handled over 900 data breaches
• The Centre for Information Policy Leadership at Hunton & Williams
• www.huntonprivacyblog.com
• www.huntonregulationtracker.com
• @hunton_privacy