21 June 2017

Cyber Security and Protecting the Supply Chain

Mel Crocker
VP, Enterprise IT and Chief Information Security Officer

Outline

- Threats relevant to Supply Chain
- What happens when supply chain attacks are successful?
- Prevent, Detect and Respond
  - How does traditional cybersecurity fit with partners?
- Questions

ENBRIDGE

Threats Abound

3 Major Cybersecurity Threats That Experts Experience Every Day

Cybersecurity Firms Warn of New Malware Threat to Electric Grids

Darktrace: IoT Is Another Insider Cyber Security Threat To Consider

Roland Moore-Colyer, June 12, 2017, 6:48 pm

Jun 14, 2017 / by Jimmy H. Koo

THE RISKY BUSINESS OF BEING OVER-EXPOSED TO ONLINE CYBERSECURITY THREATS

Cyber security employee shortage barrier to effective threat detection

Feature 31 MAY 2017

Panel urges quick, decisive action on cybersecurity

SEC identifies adviser cyber security flaws

Privacy & Security

WannaCry and now EternalBlue threats prove cybersecurity review is a must

First National Technology Solutions says software updates, constant patching and employee education are musts.

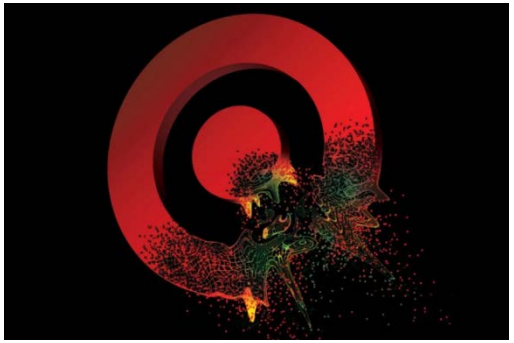
ENBRIDGE

Threats executed through partners – Target - 2013

How the Hackers Broke In

1. They probably used credentials of an HVAC vendor to get into Target's network, spending weeks on reconnaissance to install a pair of malware programs.
2. The hackers sent credit card number-stealing malware to cashier stations in all domestic Target stores.
3. They also installed malicious code that sent card data to three hijacked "staging point" servers in the U.S. before the data headed to Moscow.
4. On Dec. 2, the credit card numbers started flowing out. Target's security system detected the hack, but the company failed to act.
5. Federal investigators warned Target of a massive data breach on Dec. 12.
6. Target confirmed and eradicated the malware on Dec. 15, after 40 million credit card numbers had been stolen.

DATA COMPILED BY BLOOMBERG; GRAPHIC BY BLOOMBERG BUSINESSWEEK



FAZIO MECHANICAL SERVICES

ENBRIDGE

What happened after the Target Breach?

- 40 million credit card numbers stolen, 110 million customers had personal data stolen
- Target spent more than $250 million responding to the breach and investigating.
- Largest holiday revenue drop in the history of the company for the holiday period, down 46% from Q4 2012 (loss of almost $500 million)
- 90 lawsuits filed by customers and banks (one settled for $10 million), some against specific board members
- Congressional inquiry

ENBRIDGE

Supply Chain Attacks

- More electronically connected every year with partners, connection = speed and connection = path for attackers
- Supply chains have become so efficient, they are often fragile, interrupt one key partner and drive large impact
- Attackers look for the weakest entry point and generally have two motivations:
  - Financial – ransomware, steal and sell
  - Disruption – terrorists – imagine disrupting the global supply chain of vehicle fuel, many attack points

Malware infecting PCs on production line, Microsoft says

Computers being infected with viruses, counterfeit software before they arrive at stores, lawsuit documents say

The Associated Press Posted: Sep 13, 2012 3:54 PM ET | Last Updated: Sep 13, 2012 7:40 PM ET

ENBRIDGE

Prevent, Detect and Respond – Expectations of Partners

- Prevent
  - Partners to do cybersecurity certification (e.g. SOC 2 Report (Service Organization Control)) as a condition of working within your supply chain.
  - Careful with the small players, cybersecurity is expensive if done well
- Detect
  - Penetration testing reports.
  - Contract can include alerting related to security incidents.
  - Depending on your organization’s maturity and the partner’s willingness, can have monitoring of access to your information on their systems.
- Respond
  - Connections active with partners to deal with incidents
  - Contractual matters in place if things get ugly

ENBRIDGE