POST-MORTEM OF A DATA BREACH

Janne Kauhanen
@jkauhanen

F-Secure Cyber Security Services
100+ ASSIGNMENTS / 3 YEARS
SERVICES PROVIDER "CORP X"

- Listed on several international stock exchanges
- Provides application services, e.g. to financial sector
- Never thought they could be targeted – "we're just a regular company"
SITUATION ONE MORNING IN SEPT 2015

- "7GB of data was sent from one financial department employees PC to IP-address xxx.xxx.xxx.xxx."

- F-Secure Labs confirmed the address as a known data exfiltration server, used in a recently activated campaign
PowerPoint slide with icons and text:

- Watering hole
- Command & Control
- Data Exfiltration
RECON

Watering hole

Command & Control

Data Exfiltration
Watering hole
Command & Control
Data Exfiltration
Watering hole

Command & Control

Data Exfiltration
EXPLOITATION

Watering hole

Command & Control

Data Exfiltration
EXPLOITATION

Watering hole

Command & Control

Data Exfiltration
ATTACK KIT DELIVERY

- Watering hole
- Command & Control
- Data Exfiltration
ATTACK KIT DELIVERY

Watering hole

Command & Control

Data Exfiltration
ATTACK KIT DELIVERY

Watering hole

Command & Control

Data Exfiltration
LATERAL MOVEMENT

Watering hole

Command & Control

Data Exfiltration
LATERAL MOVEMENT

Watering hole

Command & Control

Data Exfiltration
LATERAL MOVEMENT

Watering hole

Command & Control

Data Exfiltration
LATERAL MOVEMENT

Watering hole

Command & Control

Data Exfiltration
DATA COLLECTION

Watering hole
Command & Control
Data Exfiltration
DATA COLLECTION

Watering hole

Command & Control

Data Exfiltration
DATA COLLECTION

Watering hole

Command & Control

Data Exfiltration
DATA COLLECTION

Watering hole
Command & Control
Data Exfiltration
DATA COLLECTION

Watering hole
Command & Control
Data Exfiltration
DATA COLLECTION

Watering hole
Command & Control
Data Exfiltration
DATA COLLECTION

Watering hole

Command & Control

Data Exfiltration
DATA EXFILTRATION

Watering hole

Command & Control

Data Exfiltration
DATA EXFILTRATION

- Watering hole
- Command & Control
- Data Exfiltration
DATA EXFILTRATION

Watering hole

Command & Control

Data Exfiltration
WHAT WAS THE BUSINESS IMPACT ON "CORP X"?
**SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE**

### Stakeholder focus & attention
- Resource demand

### Discovery
- **Short-term implications**
  - Loss of efficiency & delivery
  - Internal reporting mayhem
  - Management’s focus on incident, not on business
  - Costs incurred in response
  - Customer interface overload

- **Incident Response**
  - IT Forensics
  - Legal & Regulatory review

- **External areas**
  - Public Relations
  - Notification management
  - Stakeholder Communication
  - Remedial Service Provision

### Long-term implications
- Loss of revenue
- Stock price effect
- Brand & Reputation damage
- Regulatory fines
- Contractual fines
- Costs incurred in remediation
- 3rd party legal liability
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Discovery, IRT-team involved
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Stakeholder focus & attention
Resource demand

Escalation to MIM
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Stakeholder notification according to the process
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

A client demands explanation;
Who, why, how, scope, remediation?
-> KAMs try to manage
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Client’s FSA’s information request
LEGAL (EXTERNAL), AND INTERNAL SEC RESOURCES TIED TO FIND ANSWERS

STAKEHOLDER FOCUS & ATTENTION

RESOURCE DEMAND
COMMS department demands info to prepare statements in advance
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

- Stakeholder focus & attention
- Resource demand

Time

External PR company involved
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

1st forensics report: The breach larger than expected
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

Stakeholder focus & attention

Resource demand

Time

Escalation to the Management Team
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

CEO: prepare a statement to BoD
Stakeholder focus & attention

Resource demand

Time

SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

IRT+MIM+CMT organization in place
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

- Client’s tender process freezed
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

CMT decision: To isolate a suspected system.
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Stakeholder focus & attention

Resource demand

Time

Reporting to client’s FSA
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

Stakeholder focus & attention vs Resource demand over Time

Several units require instructions from CMT
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

- Stakeholder focus & attention
- Resource demand

Time

Closed accounts hinder internal operations
SIMPLIFIED CYBER BREACH'S BUSINESS IMPACT TIMELINE

- Stakeholder focus & attention
- Resource demand

Time

Major Security Improvement program initiated
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Stakeholder focus & attention

Resource demand

Time

Improvement program scoping

F-Secure
SIMPLIFIED CYBER BREACH’S BUSINESS IMPACT TIMELINE

Time

Resource demand

Stakeholder focus & attention

Today
SUMMARY

- Succesfull business makes you a potential target
- This case was a textbook example
- Although prepared, the level of business disruption came as a surprise
- You have firedrills – why not cyberdrills?
HOW TO PREVENT A DATA BREACH

Marko Finnig
ON AVERAGE IT TAKES TOO LONG TO REACT TO A BREACH
LETS LOOK AT HOW ATTACKERS OPERATE AND WHAT THEY ARE AFTER

FOOTHOLD
- User credentials
- Operating environment
- Operating system

OBJECTIVE
- Data
- Control

Criminals
Hacktivists
Industrial espionage
Nation states
IN THE PROCESS, THEY WILL ALWAYS LEAVE (SOMETIMES VERY SUBTLE) FOOTPRINTS

**FOOTHOLD**

- Criminals
- Hacktivists
- Industrial espionage
- Nation states

**USER CREDENTIALS**

- Operating environment

**OPERATING SYSTEM**

- Windows
- Apple
- BlackBerry

**FOOTPRINTS**

- User level footprints
- Application level footprints
- Network level footprints
- Operating Environment footprints
- OS level footprints
2 COMMON WAYS TO GAIN FOOTHOLD ARE VIA PUBLIC FACING EMPLOYEES AND (FORGOTTEN) SERVERS

ATTACKER

FOOTHOLD

(PR, Sales & Marketing, HR, internet facing servers)
99,9 % DO LITTLE DAMAGE

0,1 % DO THE MOST DAMAGE
Usually well covered by the current security solutions in organizations

• Address machine conducted attacks
  • Phishing & exploit (email as vector)
  • Ransomware
  • 99.9% of the malware

• Solutions (Prevent):
  • Firewall
  • Email security
  • End-point protection
  • ..

Usually not covered at all by the current security solutions in organizations...

• Address human conducted attacks
  • Spear-Phishing & exploit (in-memory backdoor)
  • Use of system internals - PowerShell, WMIC, Service Commands ...
  • Use of remote admin tools (RAT) and hacking tools – Orcus, Litemanager, LuminosityLink, Mimikatz
  • Hide command & control traffic – Office365, GMail, HTTPS

• Solutions (Detect & Respond):
  • Managed Detection and Response (end-points)
EXPAND YOUR CAPABILITIES TO DETECT TECHNIQUES TACTICS PROCEDURES USED BY SKILLED ADVERSARIES

Prevention
Detect & Respond

TTP categories
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

ATT&CK™

MITRE
PREVENTION AND DETECTION & RESPONSE APPROACHES ARE FUNDAMENTALLY DIFFERENT

PREVENTION:
- Defenders dilemma: Be right every time, attacker needs to be right only once. Products can be bought and tested by the attacker.

DETECTION & RESPONSE:
- Attackers dilemma: Be right every time, defender needs to be right only once. Services cannot be bought and tested by the attacker.
HOW DO YOU EVALUATE ALL THESE OPTIONS?
..OR HOW DO YOU EVEN KNOW HOW GOOD YOUR EXISTING DEFENCES ARE?
THE ONLY WAY TO KNOW FOR SURE IS TO RUN DRILLS
SEPARATE THREAT ACTORS INTO GROUPS TO SUPPORT INVESTMENTS

Causing Most Damage

- Nation States
  - Most commonly seen as impossible and too expensive to address, those address these are the ones cannot afford not to

- Organized Cyber Crime
  - Risk cannot be removed, to be addressed with cyber security approach, GDPR & NIS as drivers.

- Cyber Crime
  - Based on customer feedback, this is the area they are investing the most: breach detection and response

- Commodity Threats
  - No major new investments here

Causing Least Damage
LARGE SHIFT FROM PREVENTION TO DETECTION AND RESPONSE APPROACHES

Gartner: By 2020, 60 percent of enterprise information security budgets will be allocated for rapid detection and response approaches.

Source: Gartner Special Report ‘Cybersecurity at the Speed of Digital Business’
SUMMARY

1. Separate threat actors in risk management to support investments
2. Map your “foothold” areas and
3. Extend your capabilities to cover TTPs (with D&R approaches)
4. Establish recurring red vs. blue drill practice
SWITCH ON FREEDOM