PREVENTION IS BETTER THAN CURE
Are our cyber adversaries winning?
FSI is one of the top 3 industries for security incidents

- Trailing only Government and Media
- Accounted for ~35% of confirmed data breaches

Verizon Data Breach Investigations Report

1.5M Accounts Exposed in Global Payments Breach

Scottrade breach exposed 4.6M customer records

Over 600M Financial Records Stolen from 2013-2015

83M Records Stolen in JPMorgan Chase Breach
Motivations may vary…

but the fact is…

**Cybercrime is now a**

£700bn+

**Booming Industry**
why are our cyber adversaries winning?
anatomy of a **data breach**
But first.... Some Terminology

- **Vulnerability**
  - A weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product

- **Exploit**
  - A piece of software, a chunk of data, or a sequence of commands that causes unintended or unanticipated behaviour to occur on software or hardware

- **Malware**
  - An umbrella term used to refer to a variety of forms of hostile or intrusive software

- **Patch**
  - Software security patches (attempt to) fix vulnerabilities that might be exploited

- **Code Execution**
  - An ability that allows an attacker to execute their own code on the victim machine

“An attacker uses an **exploit** against a **vulnerability**, on an **unpatched** system, to obtain **code execution**, often resulting in the installation of **malware**”
Step 1: Reconnaissance

Identify a specific target within an organisation:

- Content from corporate websites
- Third-party sites to identify key targets
- Common search techniques
Step 1: Reconnaissance

Simple Google Search
filetype:xls inurl:attendees

Event attendee contact details
Step 1: Reconnaissance

Identify the tools used to protect an organisation

Checkpoint Firewall Expert - Info Security Sr Advisor
States

This Firewall Engineer is an expert with CheckPoint firewalls and maintains enterprise information security policies, technical standards, guidelines,

Experience

Sr IT Security Analyst

Significantly increased Web Security by engineering and installing FireEye Web Malware Protection System devices across the enterprise resulting in immediate detection of zero day malware attacks on the network.
Step 2: Weaponisation & Delivery

- **Spear Phishing**: Attack a with a specific target
- **Watering Hole**: Attack a group with specific interests
- **Everything Else**: USB stick, direct network attack etc
Step 2: Weaponisation & Delivery: Spear Phishing + Drive-by Download

1. Targeted malicious email sent to user

2. User clicks on link to a malicious website

3. Malicious website silently uses exploit kit against a client-side vulnerability

4. ‘Drive-by download’ of malicious payload

5. System infected, attacker has full access
Step 2: Weaponisation & Delivery: Watering hole + Drive-by Download
Step 2: Weaponisation & Delivery

Ooh – a USB stick!

I wonder what’s on it...
Step 3: Exploitation

Exploiting the user

Why use malware when you have legitimate credentials?

Users are typically the path of least resistance
Step 3: Exploitation

Exploiting software

Why use a valuable, previously unknown exploit (aka ‘0-day’) when old vulnerabilities may not be patched?
Step 4: Installation

Myth

Highly customised and unique tools are used for most attacks

Reality

‘Off-the-shelf' tools are most commonly used in an attack
Step 4: Installation

- Keylogger
- Audio Capture
- Screen Capture
- Webcam Capture
Step 4: Installation

Buy ready-made, malicious software with 2 years support for only $140!
Step 4: Installation

Or buy a massive, ready-made malware network for $15k!
Step 5: Command and Control (aka ‘C2' or ‘CnC’)

Communicating with infected hosts and providing instructions
Step 5: Command and Control (aka ‘C2' or ‘CnC’)

2\textsuperscript{nd} stage malware download and establish C2 channel
Step 6: Actions on Objectives

C2 ultimately enables the attacker’s endgame: Actions on Objectives

- Steal local credentials
- Dump domain credentials
- Steal local information
- Steal repository information
- Information exfiltration
- Objective based commands
- Deface or host malware from site
Step 6: Actions on the Objective

Goals Inside the Network

Completed by an Active Operator

Your data in their hands
Prevention Opportunities in the Cyber Attack Lifecycle

1. Reconnaissance
2. Delivery
3. Exploitation
4. Installation
5. Command-and-Control
6. Objective

Unauthorised Access

Unauthorised Use
…so what have we been doing wrong?
Legacy Whack-a-Mole Security
We mistakenly shift focus to detection and remediation

“The Home Office has determined that preventing attacks on our streets is futile and is therefore shifting investment to crime scene cleanup and timely restoration of normal life"
a new approach to prevention
1: Be Positioned to Prevent

- On the Endpoint, anywhere it resides
- At the Internet Edge and Partner Edge
- Between our Employees Devices inside the network
- At the Data Centre Edge and between servers
- Within Private, Public, Hybrid Clouds and SaaS platforms

‘Zero Trust’ Approach
2: On the Endpoint: Prevent the Techniques - not the Attacks

**Individual Attacks**
- 1,000s
  - New Software Vulnerability Exploits p/a

**Core Techniques**
- 2-4
  - New Exploitation Techniques p/a

**Individual Attacks**
- 1,000,000s
  - New Malware variants p/a

**Core Techniques**
- ~10s
  - New Malware Techniques p/a

Signature-based, AV technology is ineffective against unknown threats
3: We need Automation

1. Prevent known threats
2. Collect for the cloud
3. Detect new threats in the cloud
4. Reprogram and disseminate
5. Prevent unknown threats
4: We must share Threat Intelligence with our peers

- Global resource for cyber threat intelligence analysis and sharing for the Financial Services industry

- Distils threat information into actionable intelligence

- Palo Alto Networks is establishing automation to consume and share threat intelligence with the FS-ISAC and its members

- Co-founded by Palo Alto Networks to share threat intelligence among cybersecurity solutions providers

- Leverage the shared intelligence to improve collective defences offered to their customers

www.securityroundtable.org - The Security Roundtable is a community designed to share best practices, use cases, and expert advice to guide executives on managing cybersecurity risks.
Only an Integrated Platform can Prevent Cyber Attacks

- On the network and on the endpoints: Positioned to Prevent
- All components natively integrated and automated
- Driven by threat intelligence in the cloud
The End Result? We disrupt the attacker’s business model.
the detail
Preventing Delivery and Installation

- **Prevent malware and exploits at the network level**
- **Deploy a solution that can detect new exploits and malware, dynamically updated your protections across AV, URL and DNS**
- **Prevent exploits that have never been seen before on the endpoint**
- **User-based policy such as limiting the download of executable files from the Internet**
- **Block commonly exploited file-types on your network**
Preventing Command-and-Control

- URL Filtering: Proactively block unknown and undesirable websites.
- Dynamic DNS: Block the Dynamic DNS URL category.
- DNS Sinkholing: Identify source of malicious DNS queries.
- Detect and Block: Common RAT C2 signatures.
## Preventing Attacks at Every Stage of the Attack Lifecycle

1. **Breach the perimeter**
   - **Next-Generation Firewall / GlobalProtect**
     - Visibility into all traffic, including SSL
     - Enable business-critical applications
     - Block high-risk applications
     - Block commonly exploited file types

2. **Deliver the malware**
   - **Traps / Sandboxing (WildFire)**
     - Block known & unknown vulnerability exploits
     - Block known and unknown malware
     - Provide detailed forensics on attacks

3. **Lateral movement**
   - **Next-Generation Firewall / GlobalProtect**
     - Establish secure zones with strictly enforced access control
     - Provide ongoing monitoring and inspection of all traffic between zones

4. **Exfiltrate data**
   - **Threat Prevention**
     - Block outbound command-and-control communications
     - Block file and data pattern uploads
     - DNS monitoring and sinkholing
   - **URL Filtering**
     - Block outbound communication to known malicious URLs and IP addresses
   - **Sandboxing (WildFire)**
     - Detecting unknown threats pervasively throughout the network

---

FINANCIAL SERVICES REFERENCE BLUEPRINT

**SaaS Protection:**
- Visibility and control
- Prevent threat propagation and data leakage

**Mobile Devices:**
- Manage and protect device, control data
- IPSec/SSL VPN

**Employee access:**
- Visibility into who accesses what
- Segmentation of departments and functions

**External Gateway:**
- Visibility and control of all Internet and external traffic
- Inspection of all traffic for known and unknown threats

**Data Center:**
- Perimeter: high performance control and inspection of all traffic
- Segmentation into zones of similar security profile

**Virtualized Data Center:**
- Gain visibility and control into East-West traffic (VM-to-VM)

**Endpoints:**
- Lightweight prevention

**Malware Analysis:**
- Cloud-based sandbox
- Auto updates to NGFW

**Endpoints:**
- Manage and protect device, control data
- IPSec/SSL VPN