Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Stats, facts & proactive defence strategies against ransomware

Patrick Wragg

Head of Incident Response

Integrity360

Amanda Spångberg

Account Manager

Integrity360

#SecurityFirstStockholm

What we are seeing..

Top initial access methods:

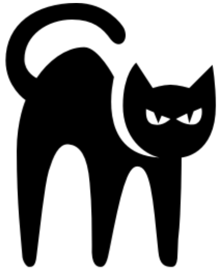
#1 - Vulnerabilities/0-days

#2 - Creds compromise

#3 - Phishing

Most skilled threat actors:

LOCKBIT 3.0



AKIRA

Notable recent threats:

CITRIX

paloalto NETWORKS

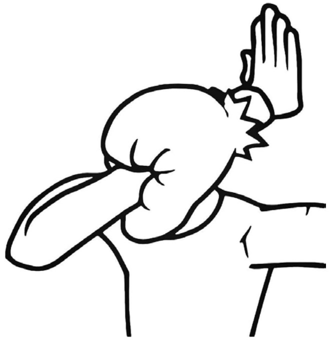
What we are seeing..

Common triage calls:

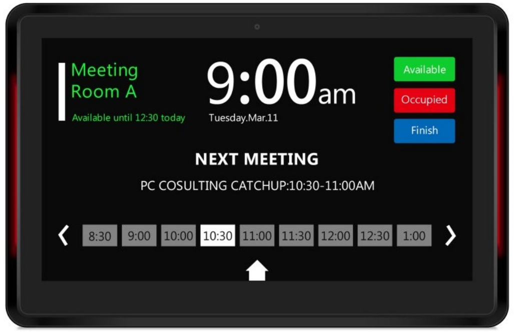
- “my mouse is moving by itself!”
- “help, someone bought guns with my cards!”
- “our website redirects to porn!”
- “our server room is flooded!”

Biggest cyber mistakes we see:

- AV in passive mode
- DC in DMZ
- Using plain FTP
- Account sharing
- Creds in spreadsheets



Most interesting case so far:



Dwell time before ransom

"How long an attacker persists within an organisation's network before being discovered"

Longest — 8 years

Average — 2 weeks

Shortest — 23 minutes

Case study

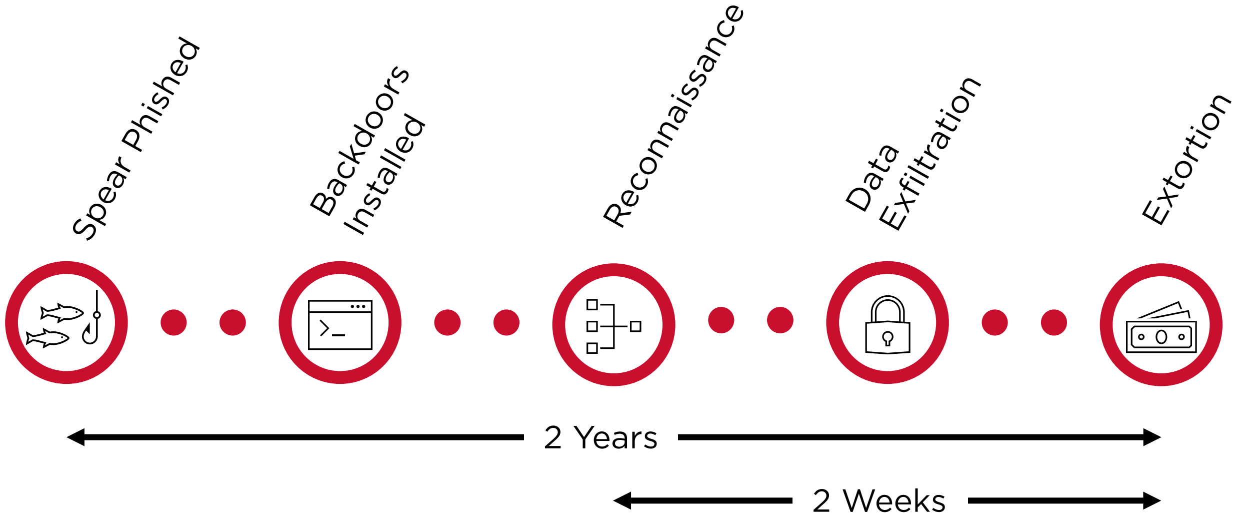
Company profile

Industry: Critical National Infra

Annual revenues: €billions

Employees: 3000

Ransomware: Black Cat



Spear Phished

Backdoors Installed

Reconnaissance

Data Exfiltration

Extortion

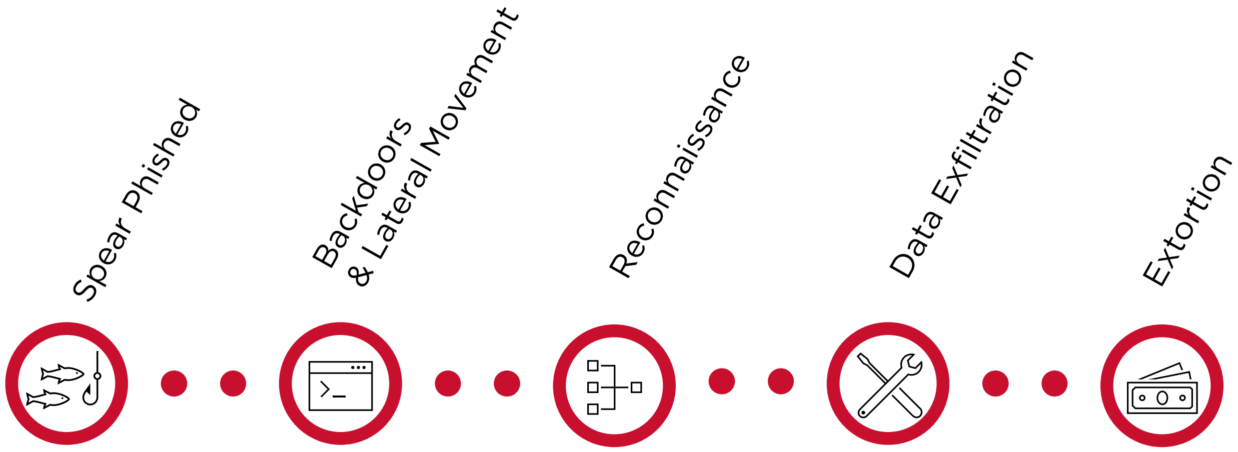
2 Years

2 Weeks

Impact

2-week business outage
€20M operational loss
Fines/Reputational Damage: €115M

Case study



Spear Phished

- HR employee gets socially engineered into opening phishing email
- Email is extremely well written and contains personal information from client
- Highly targeted

Backdoors & Lateral Movement

- SDBbot, a backdoor that maintains persistence via Shim Databases installed as initial backdoor
- Cobalt Strike then deployed to over 30 core servers over the next 6 months

Reconnaissance

- 18 months in, activity becomes heavy and frequent
- TA finds credentials stored in plaintext spreadsheets and OT SCADA diagrams

Data Exfiltration

- Exfiltration of 10TB uploaded via Rclone exfiltration tool to Mega.io
- SQL database dump attempt causes a database crash, alerting the client

Extortion

- Ransom note sent to executives demanding £50m
- TA threatens to go public and say they can control the industrial control systems and cause harm to the public
- TA phones employee's personal phones and threatens their family

Case study - Lessons to learn

Credentials

Credentials (including Domain Administrator) were kept in plaintext spreadsheet

Response

Lack of response plan led to panic & blame, slowing response efforts

Monitoring

What controls did detect behaviour were not monitored, leaving attacker to go undetected

Segmentation

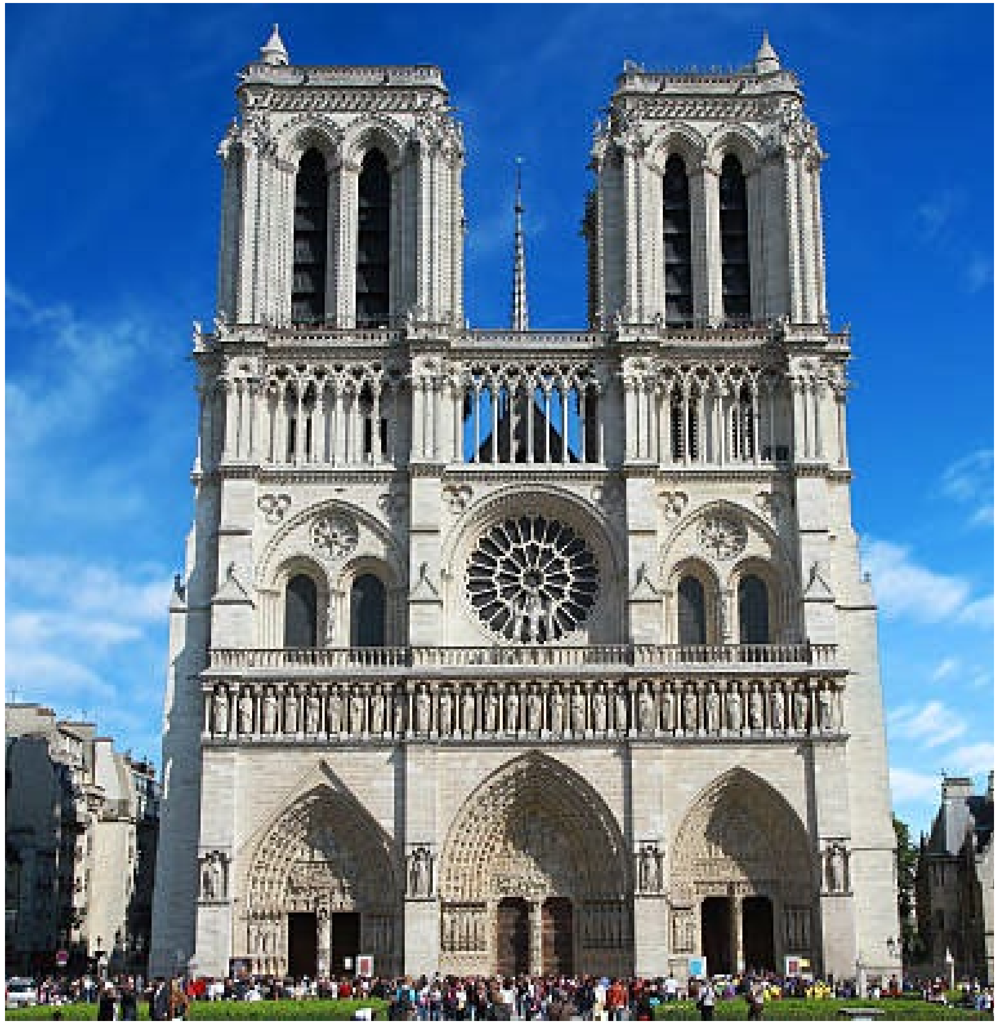
Lack of proper segmentation in the environment meant that lateral movement was trivial

Logging

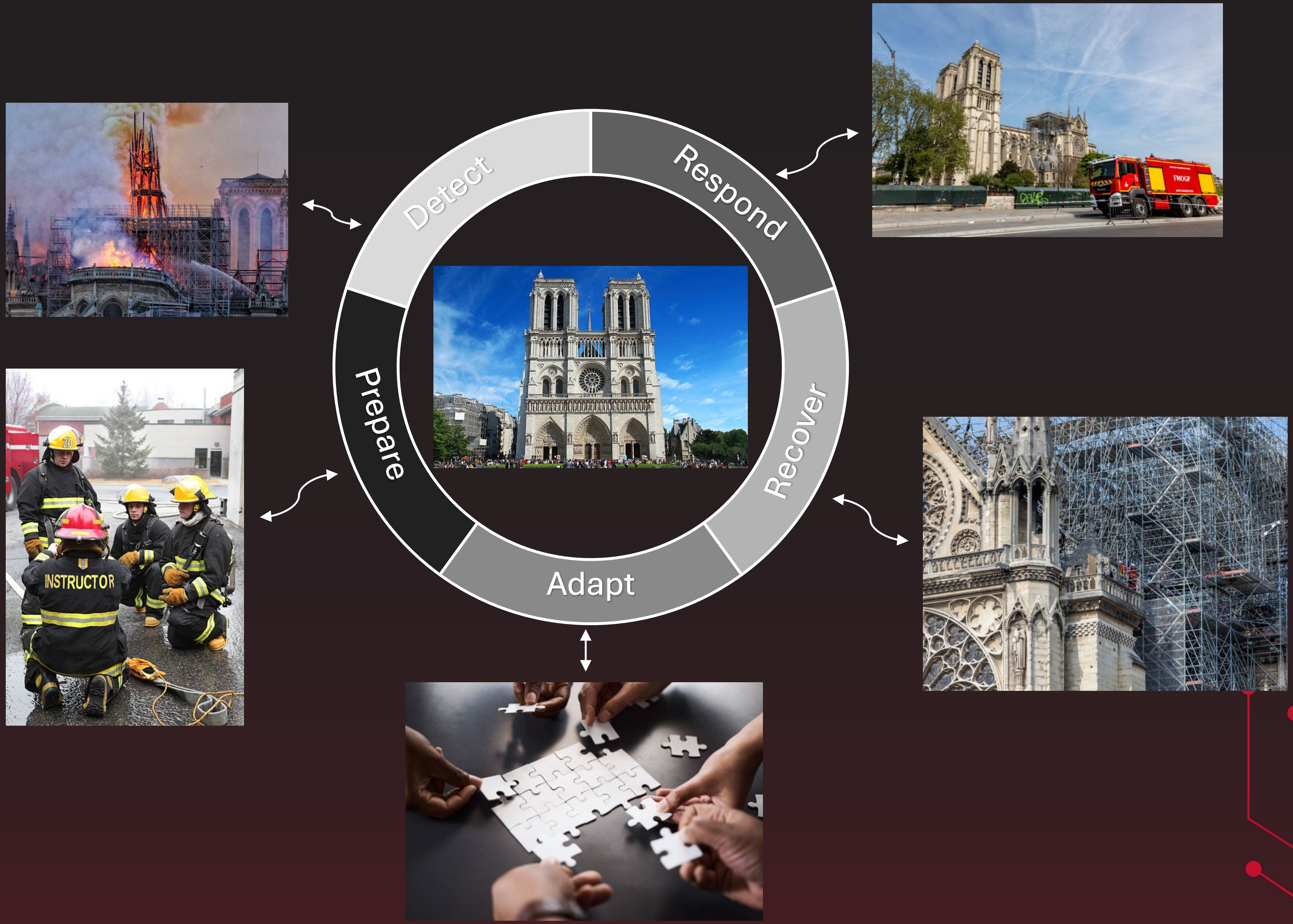
- Lack of sufficient logging made forensics difficult.
- Coverage of devices was bad

Legacy Equipment

- Legacy devices meant that forensics was more difficult
- Post-incident recovery difficult due to legacy software



Do you know this building?



Detect

Respond

Recover

Adapt

Prepare

Integrity360
your **security** in mind

Thank you

Patrick Wragg
patrick.wragg@integrity360.com

Amanda Spångberg
amanda.spangberg@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstStockholm