Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Stats, facts, and proactive defence strategies against ransomware

Patrick Wragg
Head of IR, Integrity360

Richard Ford
Chief Technology Officer, Integrity360

#SecurityFirstDublin

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Our IR stats...

Top initial access methods:
#1 Unpatched Vulnerabilities
#2 Credential Compromise
#3 Phishing Emails

Most interesting breach:
Android firmware rootkit

Average data exfiltrated:
2TB

Most common vulnerabilities:
CITRIX ivanti ATLASSIAN

Our most common adversaries:
1. Lockbit
2. Black Basta
3. Alphv (Blackcat)

#1 Motivation
Money

Time before a company realises it's compromised:
- Shortest: 23 minutes
- Average: 2 weeks
- Longest: 8 years

Biggest cyber mistakes we've seen:
- AV in passive mode
- DC put in DMZ
- Using plain FTP
- Account sharing
- Passwords stored in excel

Common triage calls we get:
- "my mouse is moving by itself"
- "help! someone is buying guns using my bank"
- "our website redirects to porn"

Case study 1

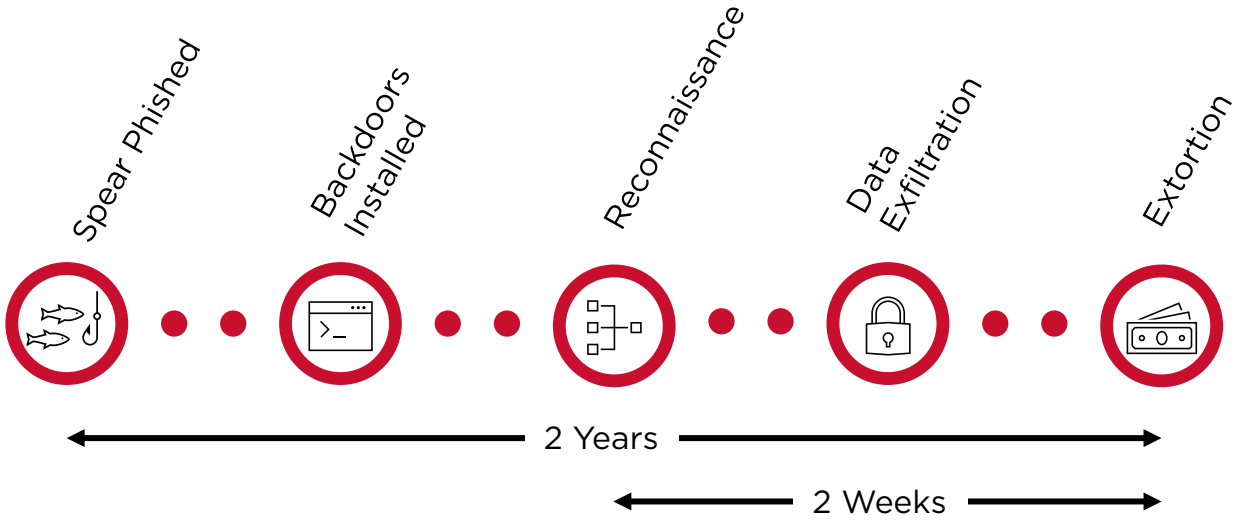
Company profile

Industry: Critical National Infra

Annual revenues: £billions

Employees: 3000

Ransomware: Lockbit



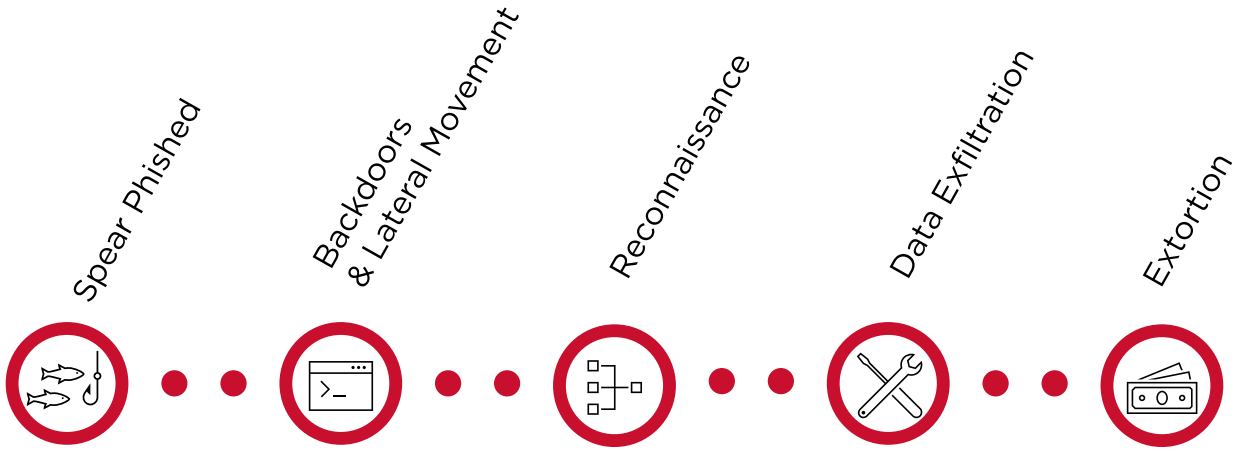
Impact

2-week business outage
£2M total cost
Fines/Reputational Damage: £60M

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Case study 1



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

- 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

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

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

- 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

Case study 1 - 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

Case study 2

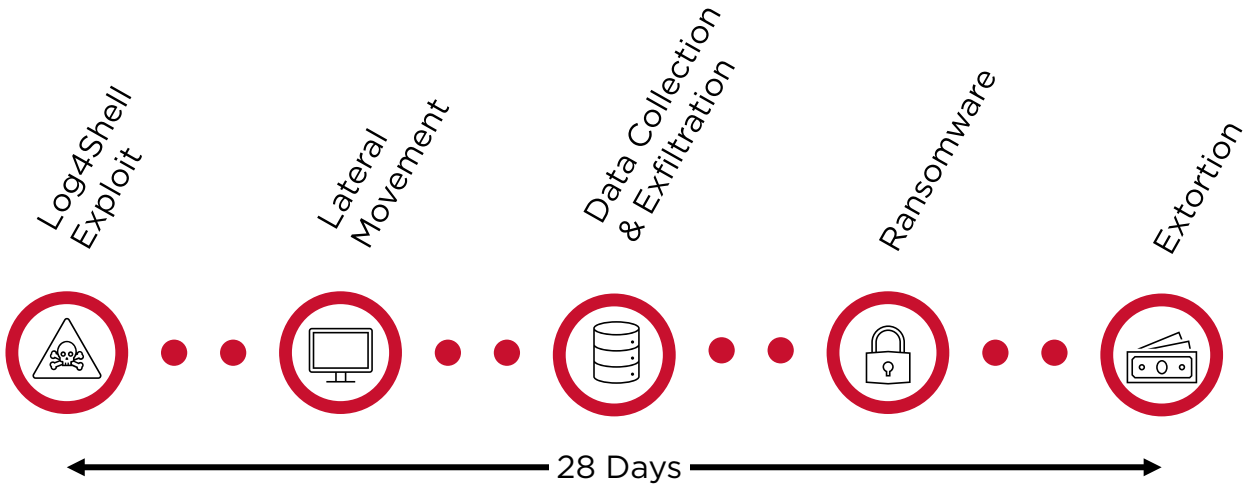
Company Profile

Industry: Energy

Annual revenues: £bn+

Employees: <2000

Ransomware: Conti



Impact

14 days business outage
PII & business sensitive data published
Reputational damage: TBD

Integrity360
your security in mind

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

Case study 2

- On-premise Microsoft Sharepoint server exposed to the Internet
- Version not classed as vulnerable by Microsoft

- Mimikatz used to obtain Domain Administrator credentials
- Cobalt Strike installed
- New user account created

- Accessed file shares
- Data uploaded to Dropbox

- Phobos ransomware deployed across whole server estate, crippling the business
- Encrypted from hypervisor down

- Ransom note left on desktops, threat to release data
- Employees personal phones called with extortion threats
- Data released to dark web a week later

Case study 2 – Lessons to learn

Patching

Common in a large number of ransomware cases, known vulnerabilities exploited due to poor vulnerability management practices

Siloed Monitoring

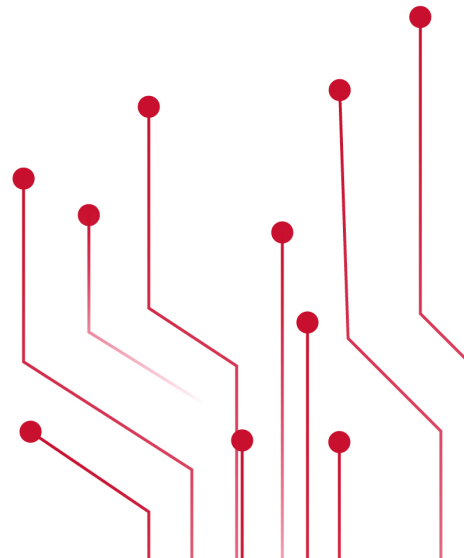
Controls did detect behaviour but were not monitored, leaving attacker to go undetected

Network Visibility

Lack of network visibility left recon & lateral movement trivial largely undetected or prevented

Response

- Low level of IR Preparedness led to slow response, increasing downtime
- No IR retainer so time was lost asking for help



Integrity360
your security in mind

Thank you

Patrick Wragg
patrick.wragg@integrity360.com

Richard Ford
richard.ford@integrity360.com

SECURITY FIRST
CYBER SECURITY CONFERENCE 2023

#SecurityFirstDublin