Premium House Lights:

The Heist

*How **customer data** was **<u>stolen</u>***

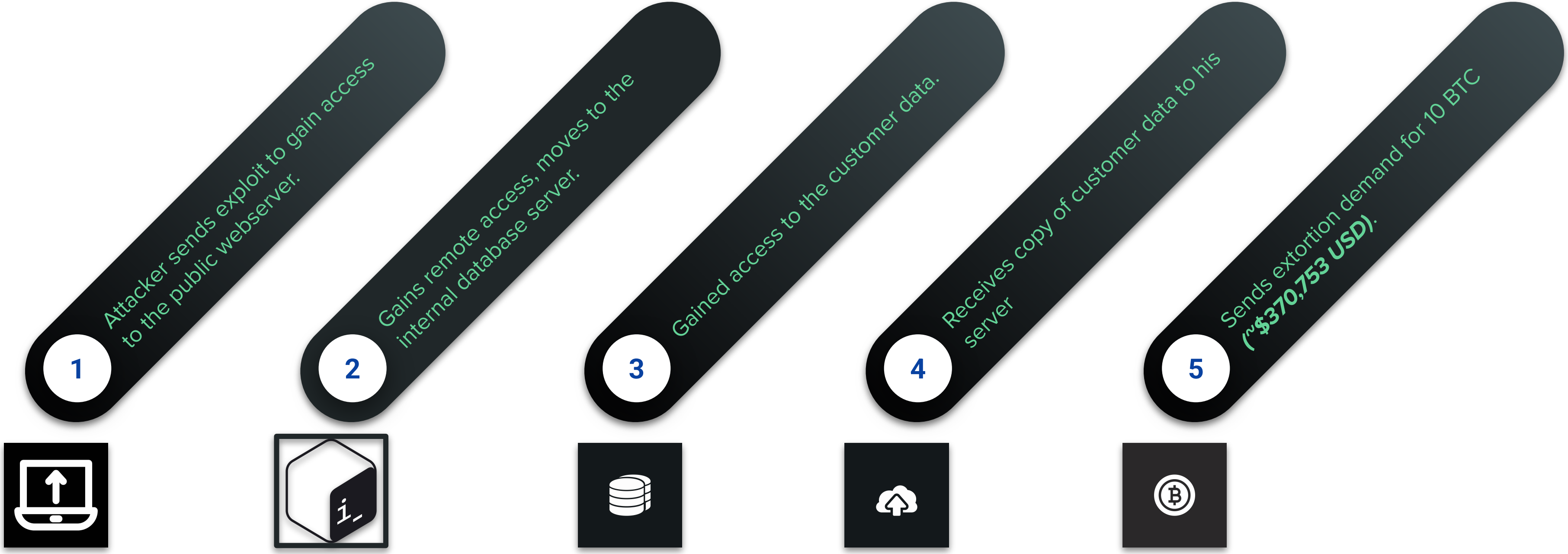
Violet Figueroa

Data Exfiltration Is
The Heist

“Data exfiltration is the unauthorized transfer or theft of sensitive company data from within the network to an external destination”
(StrongDM, 2024; Fortinet, 2025).

The Heist of personal data leading to
financial loss, regulatory penalties, and reputational harm.

The Plan



1. Attacker sends exploit to gain access to the public webserver.
2. Gains remote access, moves to the internal database server.
3. Gained access to the customer data.
4. Receives copy of customer data to his server
5. Sends extortion demand for 10 BTC ***(~$370,753 USD)***.

The Takeaways Of The Heist

- 244 customer records stolen: *Names, addresses, financial data*
- Ransom demand: *10 BTC (~$370,753 USD)*
- Consequences:
  a. Regulatory exposure *(GDPR, PCI DSS)*
  b. *Customer trust* and reputational damage
  c. Potential *business disruption*

How The Heist Happened

1 Initial Access (Get In)

Unrestricted file upload vulnerability on public webserver (10.10.1.2)

2.1 Lateral Movement (Find The Goods)

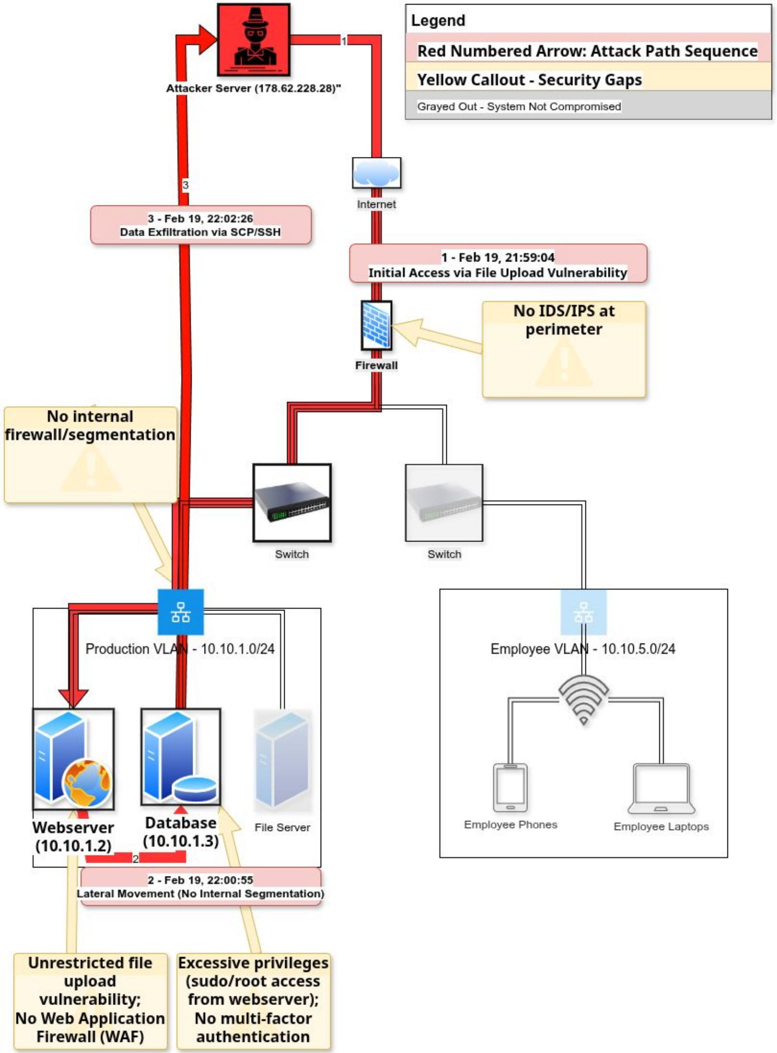
No internal segmentation allowed direct access to database (10.10.1.3)

2.2 Privilege Escalation (Say You're The Boss)

Excessive sudo privileges enabled complete database access

3. Data Exfiltration (Take The Goods)

244 records extracted via SCP to external attacker server


Legend
Red Numbered Arrow: Attack Path Sequence
Yellow Callout - Security Gaps
Grayed Out - System Not Compromised
Attacker Server (178.62.228.28)"
1
3
Internet
3 - Feb 19, 22:02:26
Data Exfiltration via SCP/SSH
1 - Feb 19, 21:59:04
Initial Access via File Upload Vulnerability
No IDS/IPS at perimeter
Firewall
No internal firewall/segmentation
Switch
Switch
Production VLAN - 10.10.1.0/24
Employee VLAN - 10.10.5.0/24
Webserver (10.10.1.2)
Database (10.10.1.3)
File Server
Employee Phones
Employee Laptops
2
2 - Feb 19, 22:00:55
Lateral Movement (No Internal Segmentation)
Unrestricted file upload vulnerability; No Web Application Firewall (WAF)
Excessive privileges (sudo/root access from webserver); No multi-factor authentication

How Do We Secure The Vault?

- To stop the next heist, we need to:
  - Segment our network with internal firewalls—so attackers can’t move freely
  - Deploy a Web Application Firewall (WAF) to block malicious uploads
  - Enforce least privilege—no more “all access” passes
  - Monitor and alert with IDS/IPS and SIEM
  - Consider Data Loss Prevention (DLP) solutions
- Proactive controls and monitoring are essential to prevent future thieves.

Key Takeaways

- Data exfiltration is *the most damaging* phase of a breach.
- Fast detection and strong controls are *critical.*
- Premium House Lights ***must act now*** to protect customer data and business reputation.