Our responsibility to you

Access our Cyber Response Support Program to guard, support and protect you.

Medibank Data Breach 2022

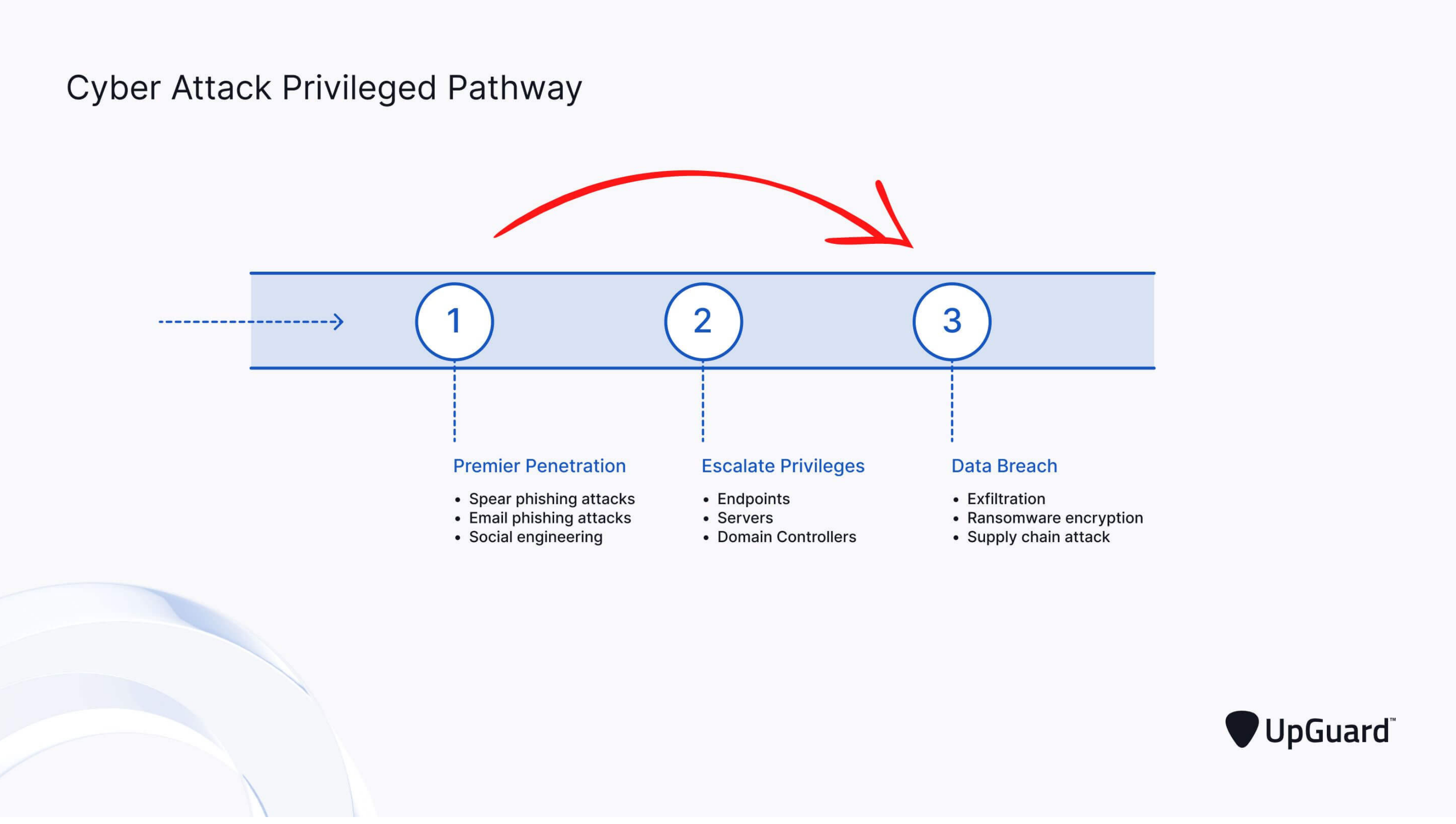
HyunOh Jeon, Jiahe Zhang, Kangning Zhang, John Antony, Michael Matta

WHAT HAPPENED

On October 13th, 2022, one of Australia's largest private health insurers, Medibank, announced a security breach. Around 200GB of personal data from about 9.7 million customers, has been stolen by a group of hackers, who are suspected to be linked with the infamous Russian hacker group REvil. This leak does not only contain private health information, but it is also personally identifiable. The attacker demanded $15 million ransom in exchange for stopping the publishing of the stolen data and returning it to Medibank. The ransom has since lowered to $9.7 million.

HOW DID IT HAPPEN

STEP 1: get access to account with privileged system access via phishing or social engineering.

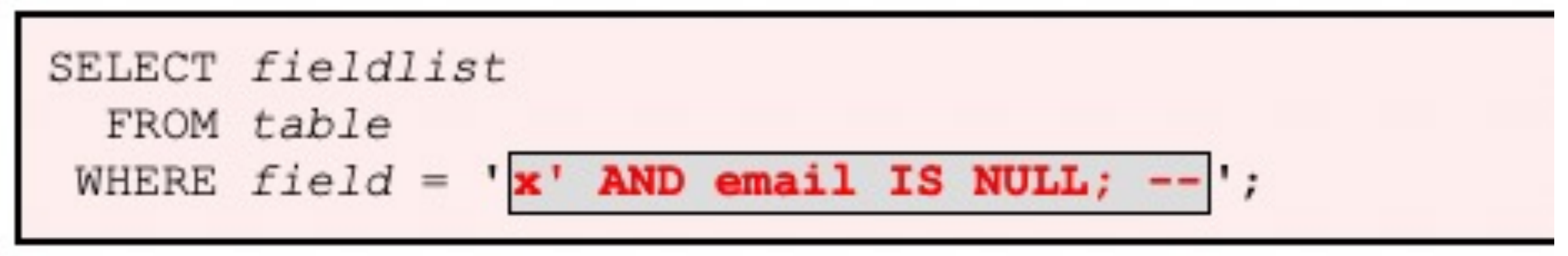


STEP 2: learn everything about the Medibank system.
It is believed that the attackers spent some time performing reconnaissance: accessing internal document to learn how the system works and how information is shared between structures.
MAC addresses and IP address of servers, routers and other devices would be helpful to navigate through the system.
Finding devices that can be used to query data and store data is also important for the next step.

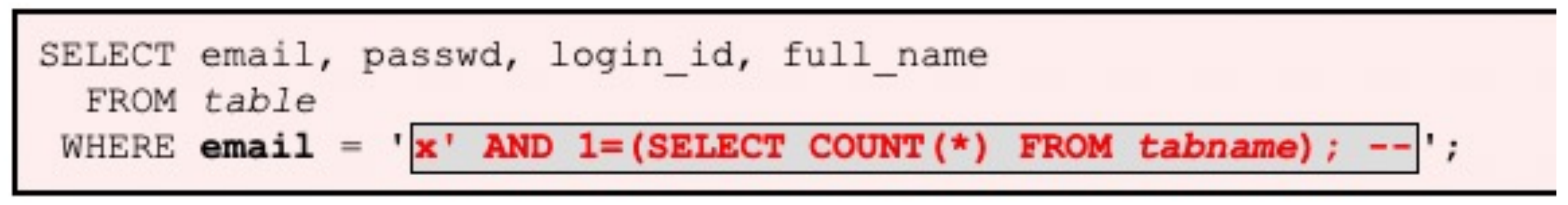
HOW DID IT HAPPEN

STEP 3: query data from the Medibank database, store the data and eventually send data out.

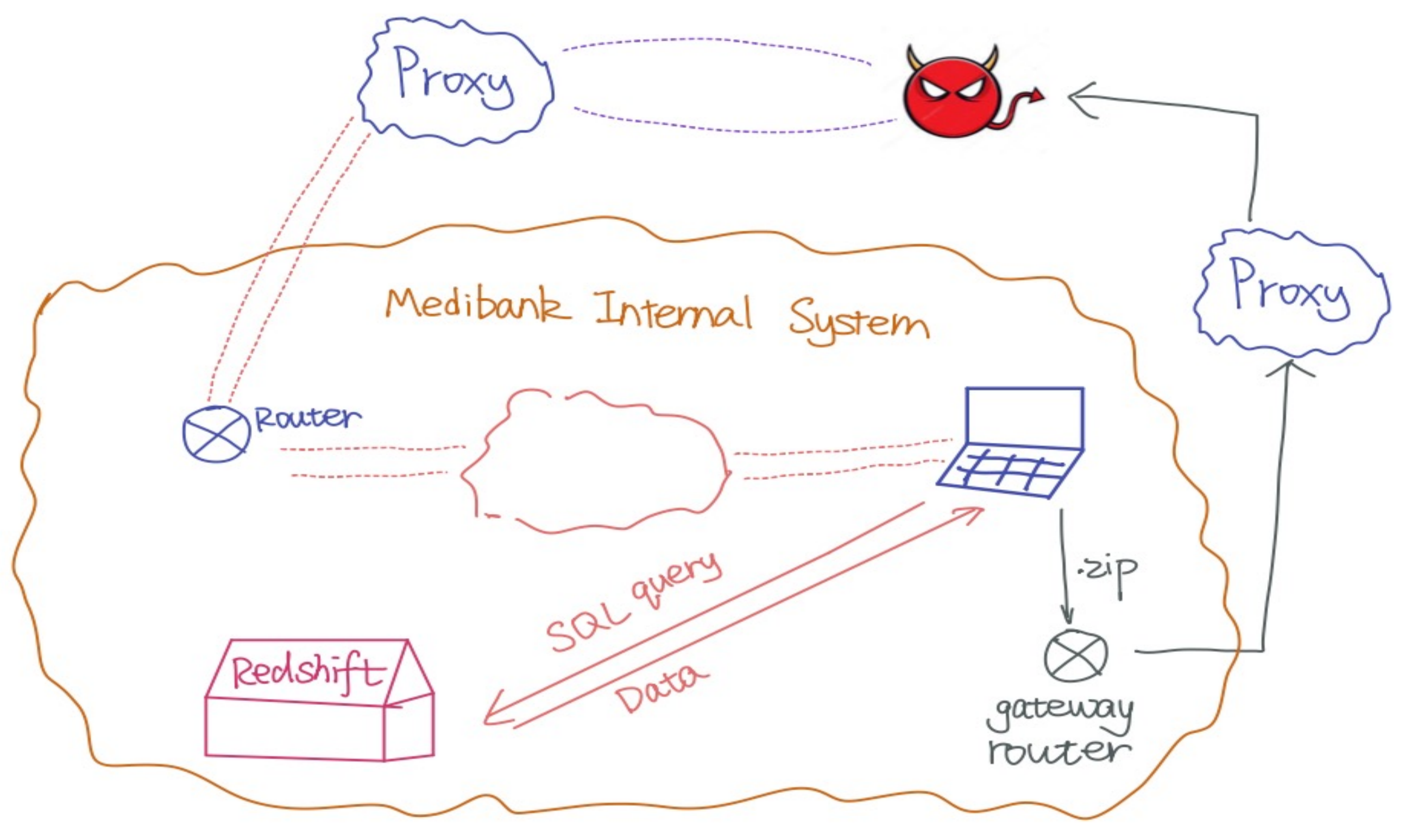
STEP 3.1: learn the data structure in the database by SQL injection.



```
SELECT fieldlist
  FROM table
 WHERE field = 'x' AND email IS NULL; --';
```



```
SELECT email, passwd, login_id, full_name
  FROM table
 WHERE email = 'x' AND 1=(SELECT COUNT(*) FROM tabname); --';
```



Step 3.2: query data and store it somewhere.

- Redshift: the data warehouse used by Medibank, uses SQL to store and analyze data.
- Gateway router (backdoor): most likely where the attacker transferred the stolen data out.
- Devices to store the stolen data: some devices inside the system to store and eventually zip the files for transfer.

WHO IS RESPONSIBLE

"… This is important because we believe that those responsible for the breach are in Russia.
Our intelligence points to a group of loosely affiliated cyber criminals, who are likely responsible for past significant breaches in countries across the world."
-AFP Commissioner Reece Kershaw

WHO IS HARMED BY THE ATTACK

- 9.7 million customers' personal information and health insurance/claims data
- People with very private health issues: files released contained "categorized" patient personal data, such as "abortion", "psycho" and so on.
- Medibank is asked to pay the $9.7 million ransom.
- Medibank stock dropped 20% after news of attack.

ETHICAL AND LEGAL ISSUES

- Fines of up to $50 million dollars, or 3 times the value of any benefit from data misuse, or 30% of the company's adjusted turnover can be issued to the company.
- The leak of huge amount of sensitive data can put public safety at risk.
- Medibank cannot trust the legitimacy of the attacker's claims of deleting the data upon paying the ransom.

WHAT COULD HAVE BEEN DONE

- Educate employees to prevent Phishing.
- Limit employees' access to the internal system to the minimum.
- Segmenting company network as well as data storage units.
- Encrypt sensitive data with distinct keys.

WHAT'S NEXT

- Medibank confirmed on November 20 that 1,496 more health records were released online.
- Medibank CEO continues to refuse to pay the ransom, believing that paying it would make Australia a bigger target for cyberattacks.
- The Australian Federal Police is investigating
- Australian government has raised penalties for data privacy violators.