# Marriott Data Breach (2018)

By: Colby & Gage

# Overview

- We will talk about:
  - What Marriott is and does
  - When was the breach
  - What was the attack
  - Phishing
  - What caused the Marriott breach
  - RAT and how it works
  - Who did the attack
  - State Sponsored Attacks

# What is Marriot

Marriott International is the world's largest and most global lodging company.

Founded almost 100 years ago

Marriott is the largest hotel chain in the world by the number of available rooms. It has 31 brands with 8,000 properties containing 1.48 million rooms in 139 countries and territories.

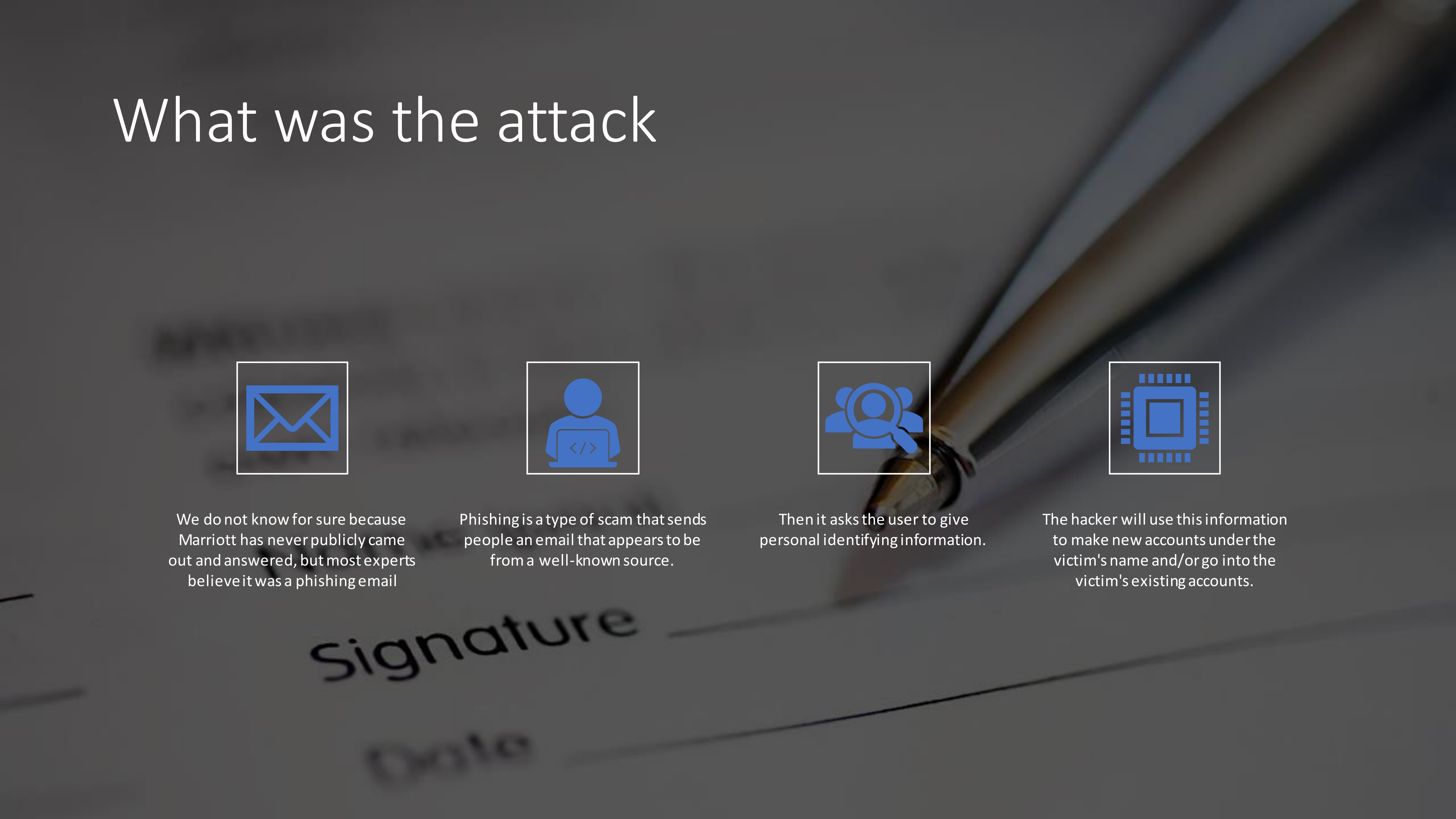
# When was the Marriot breach

On Sept. 8, 2018, an internal security tool flagged a suspicious attempt to access the internal guest reservation database. This flag caused an internal investigation. After the investigation it was found that it was breached back in 2014.

Marriott found the attackers had encrypted data and tried to remove it from the system.

By November they were able to decrypt the data and found that it included up to 500 million guest records. Including credit card and passport number

# What was the attack



We do not know for sure because Marriott has never publicly came out and answered, but most experts believe it was a phishing email

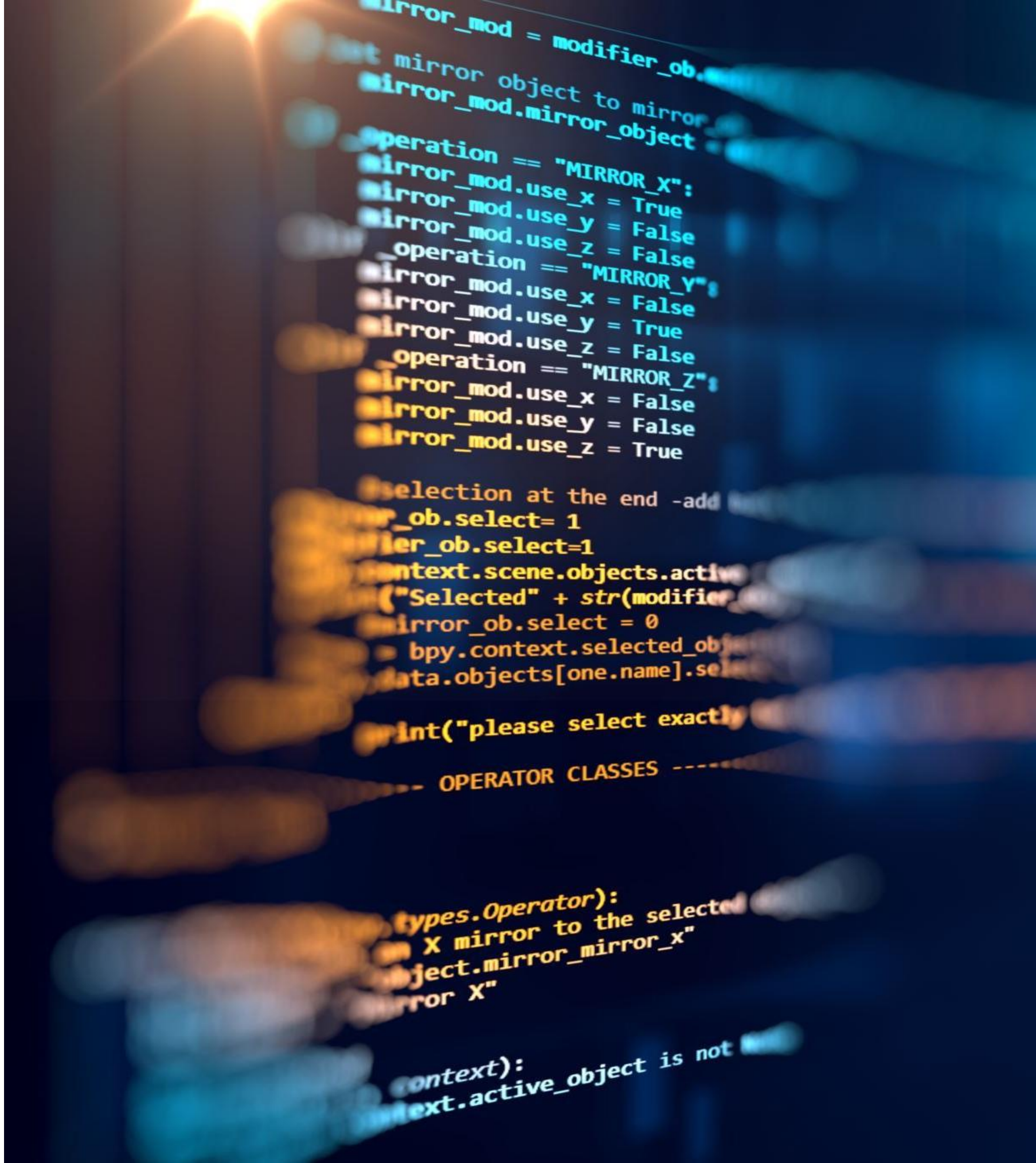
Phishing is a type of scam that sends people an email that appears to be from a well-known source.

Then it asks the user to give personal identifying information.

The hacker will use this information to make new accounts under the victim's name and/or go into the victim's existing accounts.

# Phishing Attack

- Phishing attacks are;
  - fraudulent emails, text messages, phone calls or web sites
- designed to trick users into downloading malware, sharing sensitive information or personal data
  - Social Security and credit card numbers, bank account numbers, login credentials

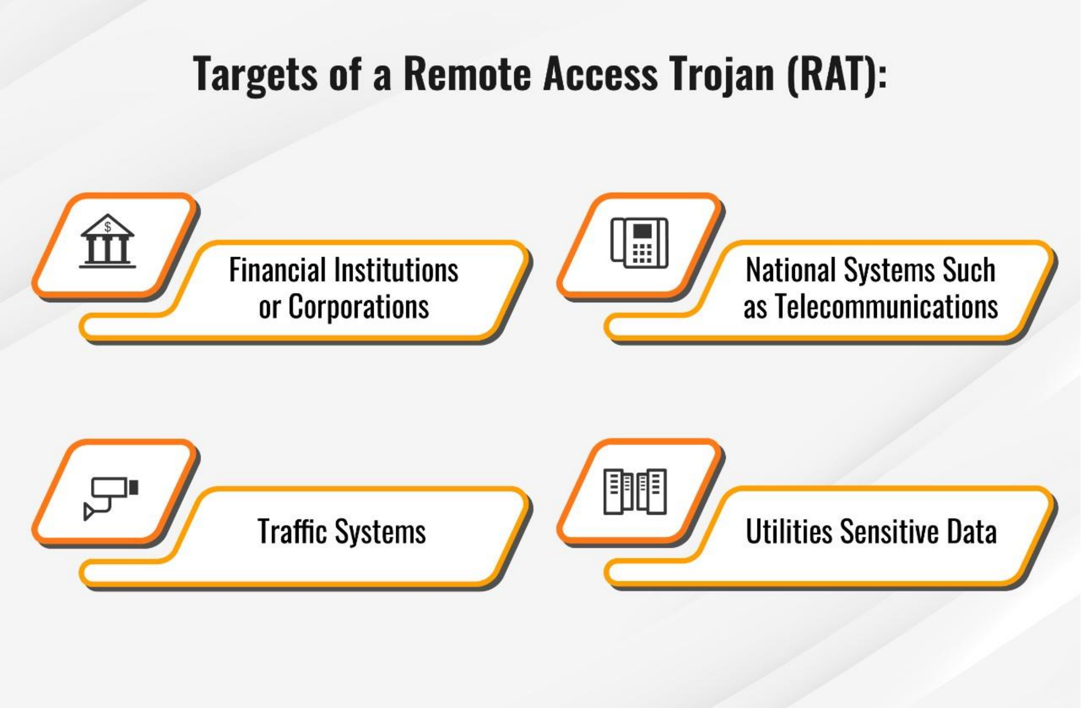


```
irror_mod = modifier_ob.
 mirror object to mirror
irror_mod.mirror_object
peration == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
_operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
_operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True

election at the end -add
_ob.select= 1
er_ob.select=1
ntext.scene.objects.activ
("Selected" + str(modifier
irror_ob.select = 0
 bpy.context.selected_ob
ata.objects[one.name].se

int("please select exactl

 OPERATOR CLASSES ----

types.Operator):
 X mirror to the selected
ject.mirror_mirror_x"
rror X"

ontext):
ext.active_object is not
```

# What caused the Mariott Data Breach

- Marriott cannot say for certain what caused the attack but can conclude the incident happened from a remote access trojan (RAT) followed with a phishing email and MimiKatz, which is a tool for sniffing out username and password combos in system memory.

- A RAT is a remote access trojan is a from of malware where it allows an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

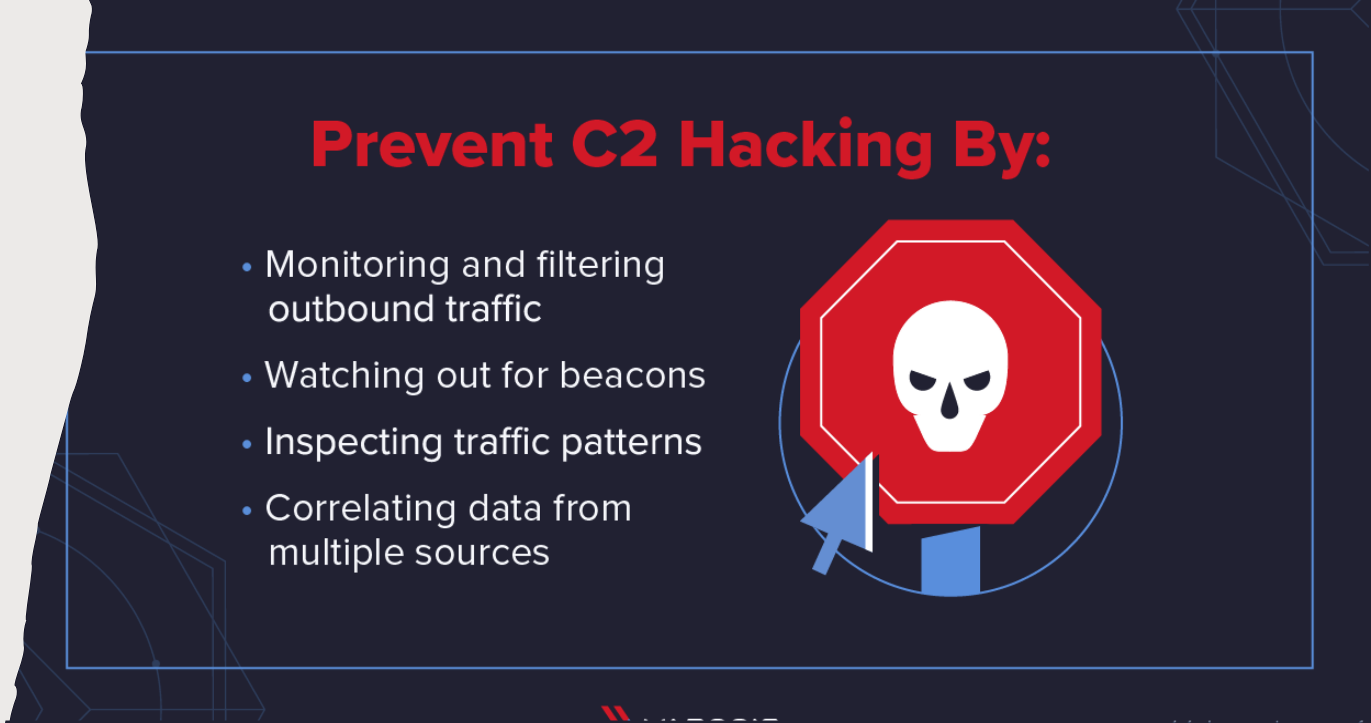


Targets of a Remote Access Trojan (RAT):

- Financial Institutions or Corporations
- National Systems Such as Telecommunications
- Traffic Systems
- Utilities Sensitive Data

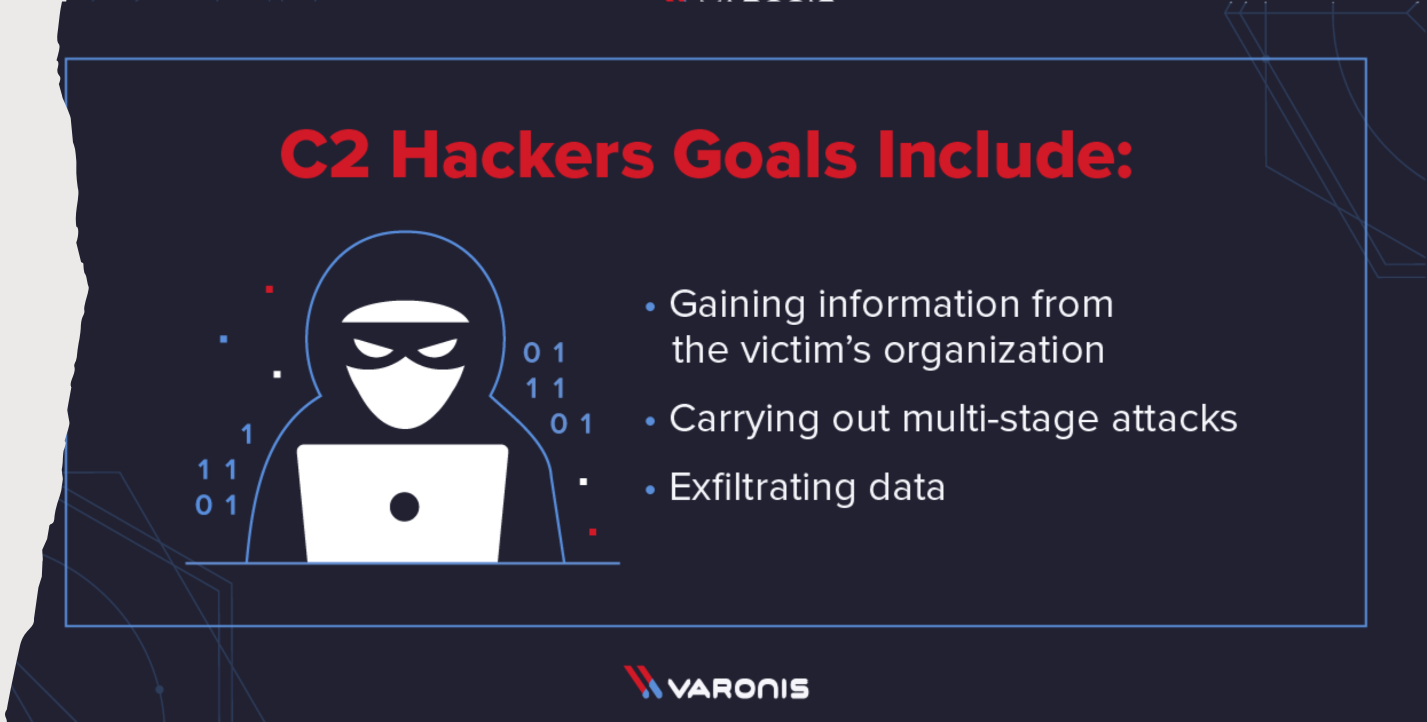
# How does a RAT work

- A RAT is designed to allow an attacker to remotely control a computer like how the Remote Desktop Protocol (RDP) and TeamViewer can be used for remote access or system administration.
- The RAT will set up a command and control (C2) channel with the attacker's server over which commands can be sent to the RAT, and data can be sent back.
- RATs commonly have a set of built-in commands and have methods for hiding their C2 traffic from detection.



## Prevent C2 Hacking By:

- Monitoring and filtering outbound traffic
- Watching out for beacons
- Inspecting traffic patterns
- Correlating data from multiple sources

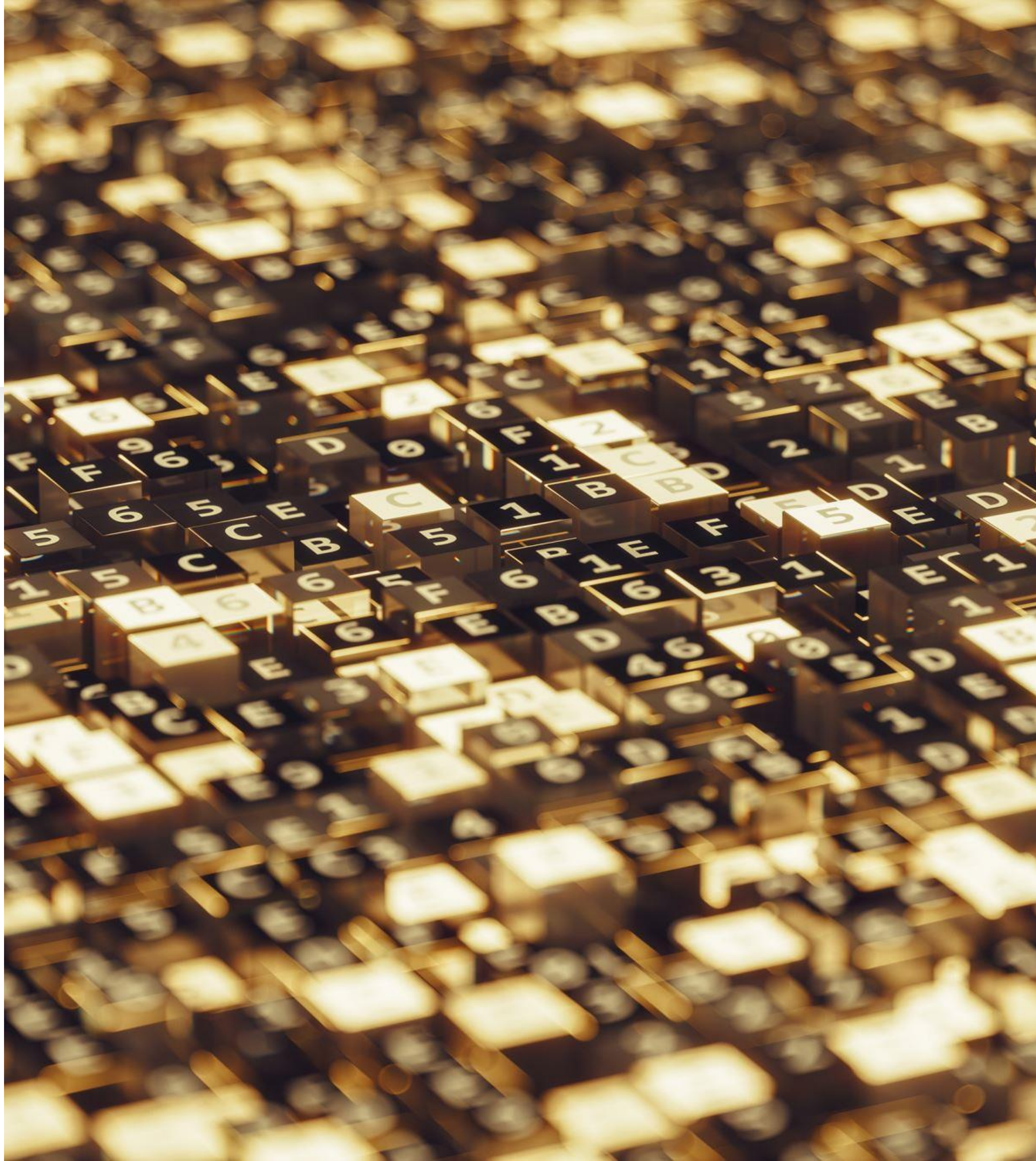


## C2 Hackers Goals Include:

- Gaining information from the victim's organization
- Carrying out multi-stage attacks
- Exfiltrating data

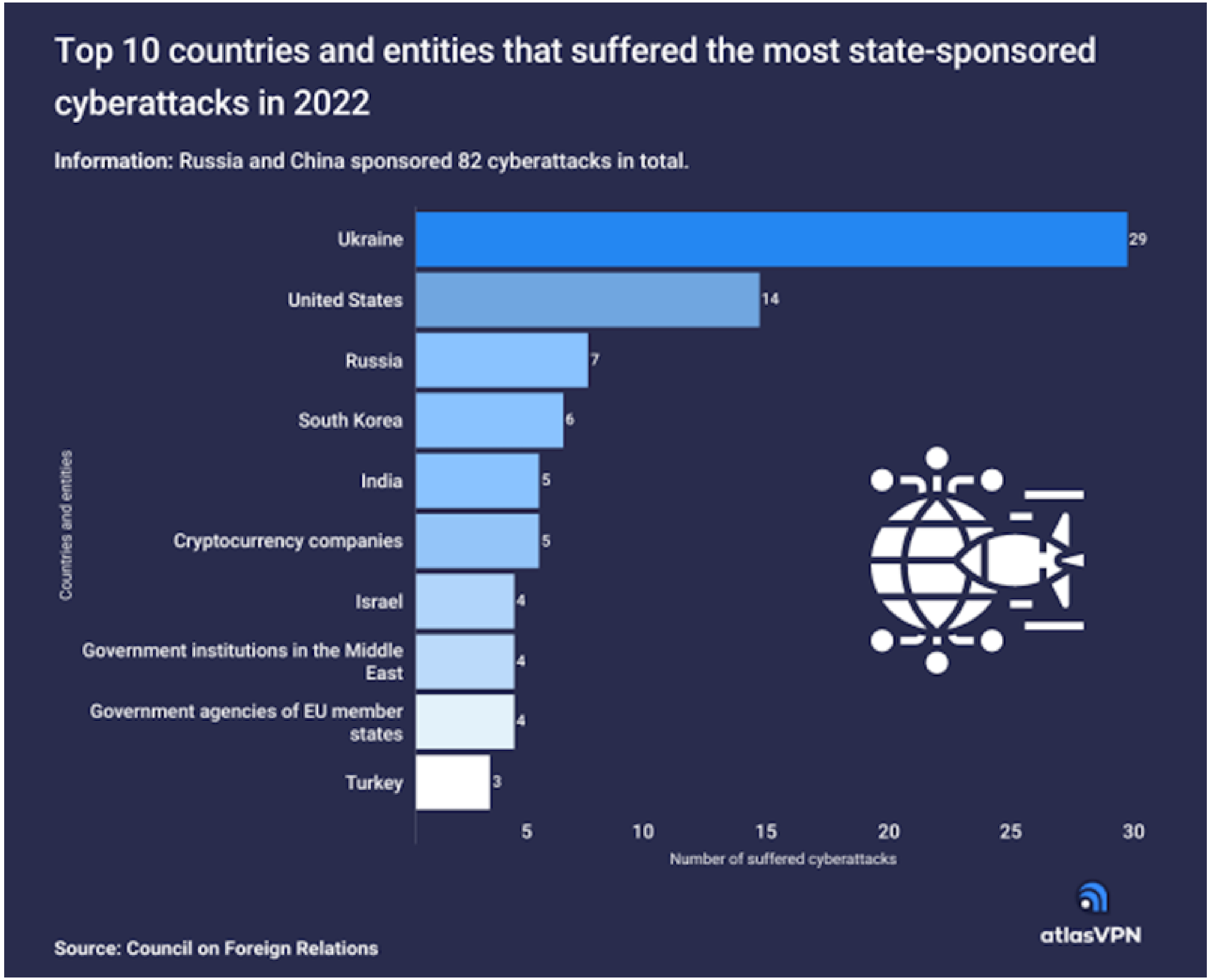
# Who did the Marriott Attack

- Unnamed sources in the U.S government says that hackers were hired by Chinese intelligence services.
- The reason for this claim is that the code and attack patterns that were used matched the techniques used by state-sponsored Chinese hackers.
- Another claim that it was a government attack was that all the information never ended up on the dark web or was held for ransom.
- The sources speculated that the reasoning behind this attack was the hope to get the information of American government employees and intelligence officers.



# State Sponsored Attacks (SSA)

- State-sponsored attacks (SSA) are carried out by cyber criminals directly linked to a nation-state. Their main goals are:
  - Identify and exploit national infrastructure vulnerabilities.
  - Gather intelligence.
  - Exploit systems and people for money.



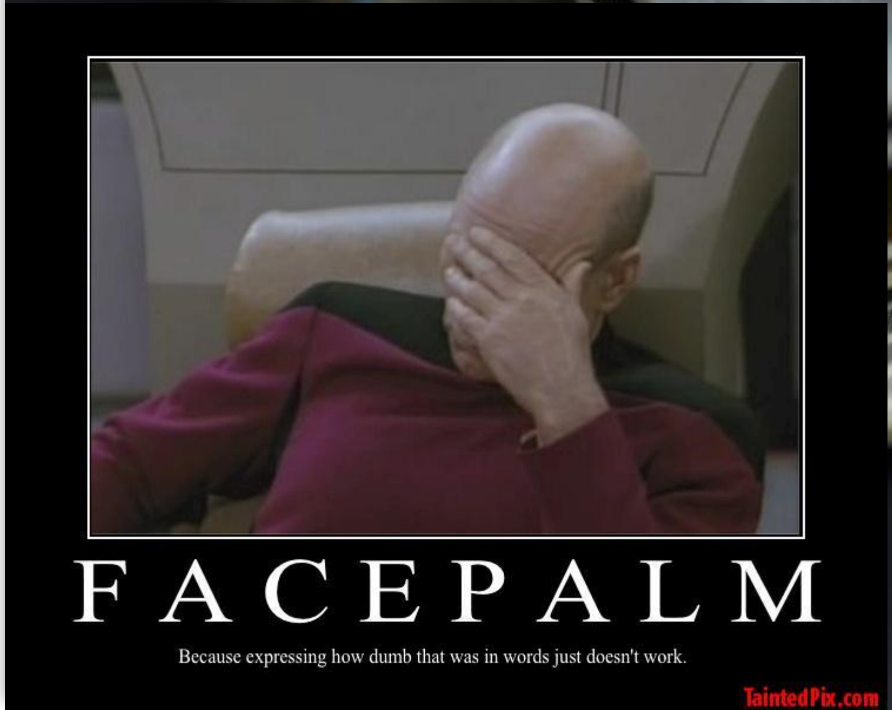
Top 10 countries and entities that suffered the most state-sponsored cyberattacks in 2022

**Information:** Russia and China sponsored 82 cyberattacks in total.

**Source: Council on Foreign Relations**

# What was the impact of Marriott Breach

- At a level, the Marriott breach was potentially catastrophic, with hundreds of millions of people's passports and credit cards stolen. Which could cause personal impacts.
- The credit card numbers were encrypted and stored BUT the encryption keys were stored on the exact same server.

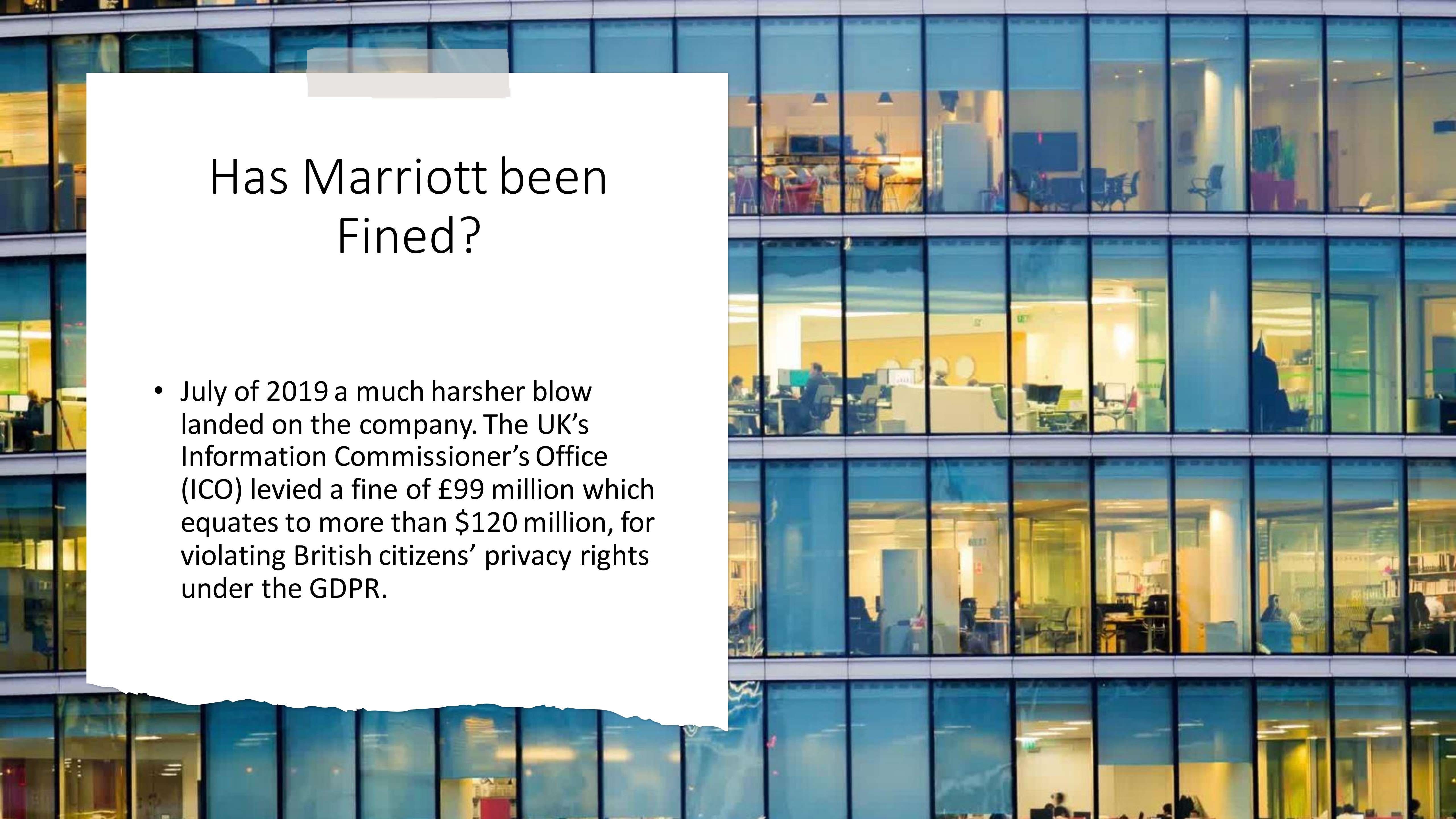

FACEPALM
Because expressing how dumb that was in words just doesn't work.
TaintedPix.com

# How Marriott Responded…poorly

- Marriott **has not** gone out of it's way to compensate any of its customers whose data was stolen.

# What did the breach cost

- The company had incurred $28 million in expenses related to breach.
- By May, the company had cut its losses to a mere $1 million.
- How? Cyber-insurance, which covered much of the initial costs associated with the crisis.

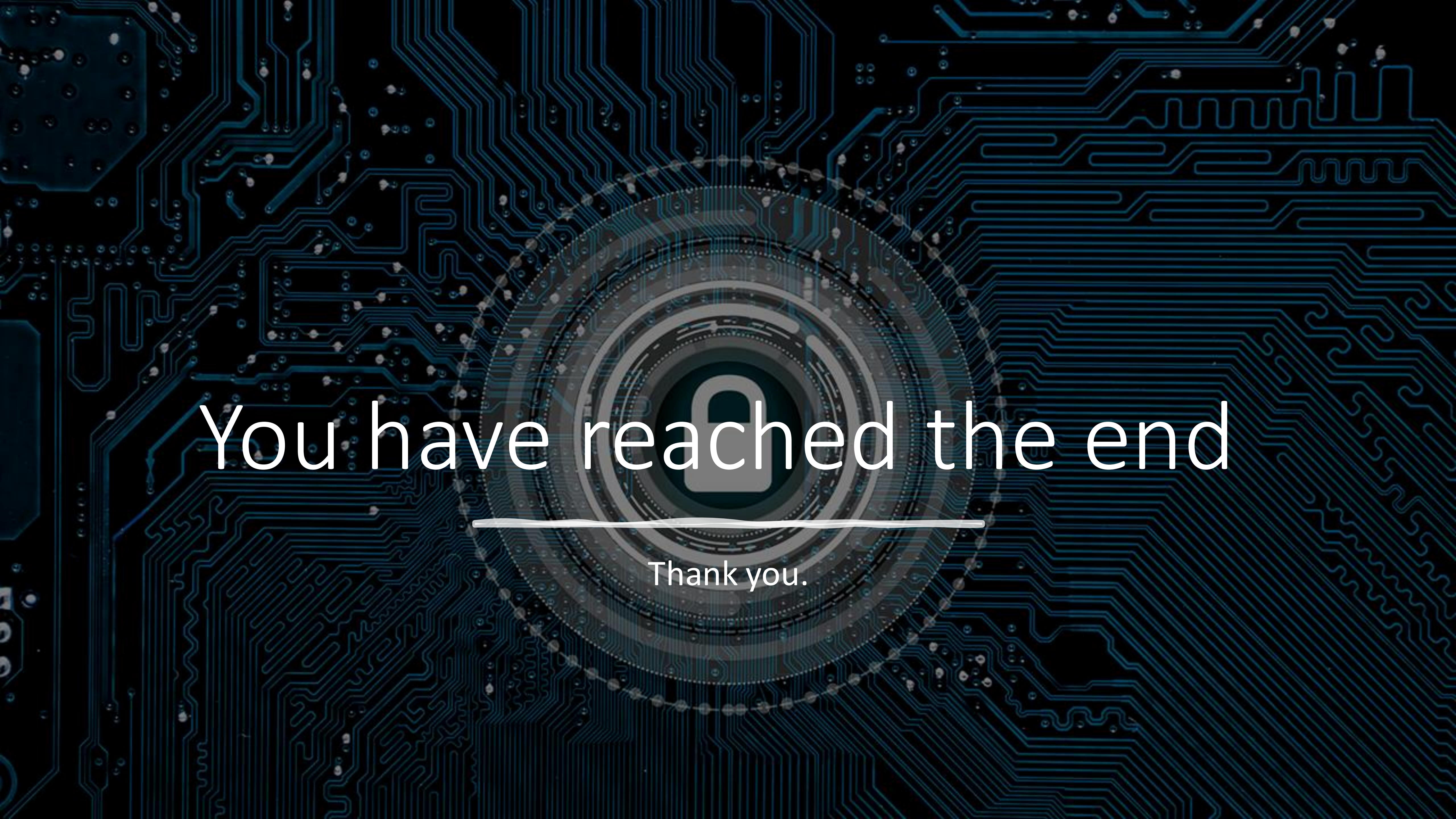


# Has Marriott been Fined?

- July of 2019 a much harsher blow landed on the company. The UK's Information Commissioner's Office (ICO) levied a fine of £99 million which equates to more than $120 million, for violating British citizens' privacy rights under the GDPR.

# Summary

- Marriott International, the largest lodging company globally, suffered a major data breach that exposed around 500 million guest records, including credit card and passport numbers, dating back to 2014.
- The breach was likely initiated through a phishing email and involved a remote access trojan and MimiKatz tool to access sensitive information.
- While Marriott suspected Chinese intelligence services were behind the attack due to the techniques used, the company did not publicly attribute the breach. The fallout was significant, potentially impacting millions of individuals and exposing encryption vulnerabilities in the stored data.
- Marriott's response, however, lacked direct compensation for affected customers, relying heavily on cyber-insurance to cover the substantial $28 million in breach-related expenses, ultimately minimizing the financial impact on the company.



# You have reached the end

Thank you.

# Cites

- https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams
- https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
- https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-remote-access-trojan/#:~:text=Remote%20access%20trojans%20(RATs)%20are,receive%20data%20back%20in%20response.
- https://www.varonis.com/blog/what-is-c2
- https://www.ibm.com/topics/phishing
- https://securanceconsulting.com/state-sponsored-attacks-and-what-they-mean-for-your-business/#:~:text=State%2Dsponsored%20attacks%20(SSA),systems%20and%20people%20for%20money.