



REMOTE INCIDENT RESPONSE IN A PANDEMIC

Joani Green



HOW DID THE PANDEMIC AFFECT CYBER SECURITY AND INCIDENT RESPONSE?

HOW DID COMPANIES RESPOND?



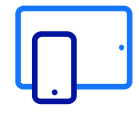
Rapid solutions
required out of
necessity



Increased use of
cloud services



Cloud transition
projects accelerated



Reliance on personal
devices



Bandwidth issues
caused networks to
topple under the
stress ->
SaaS opened up

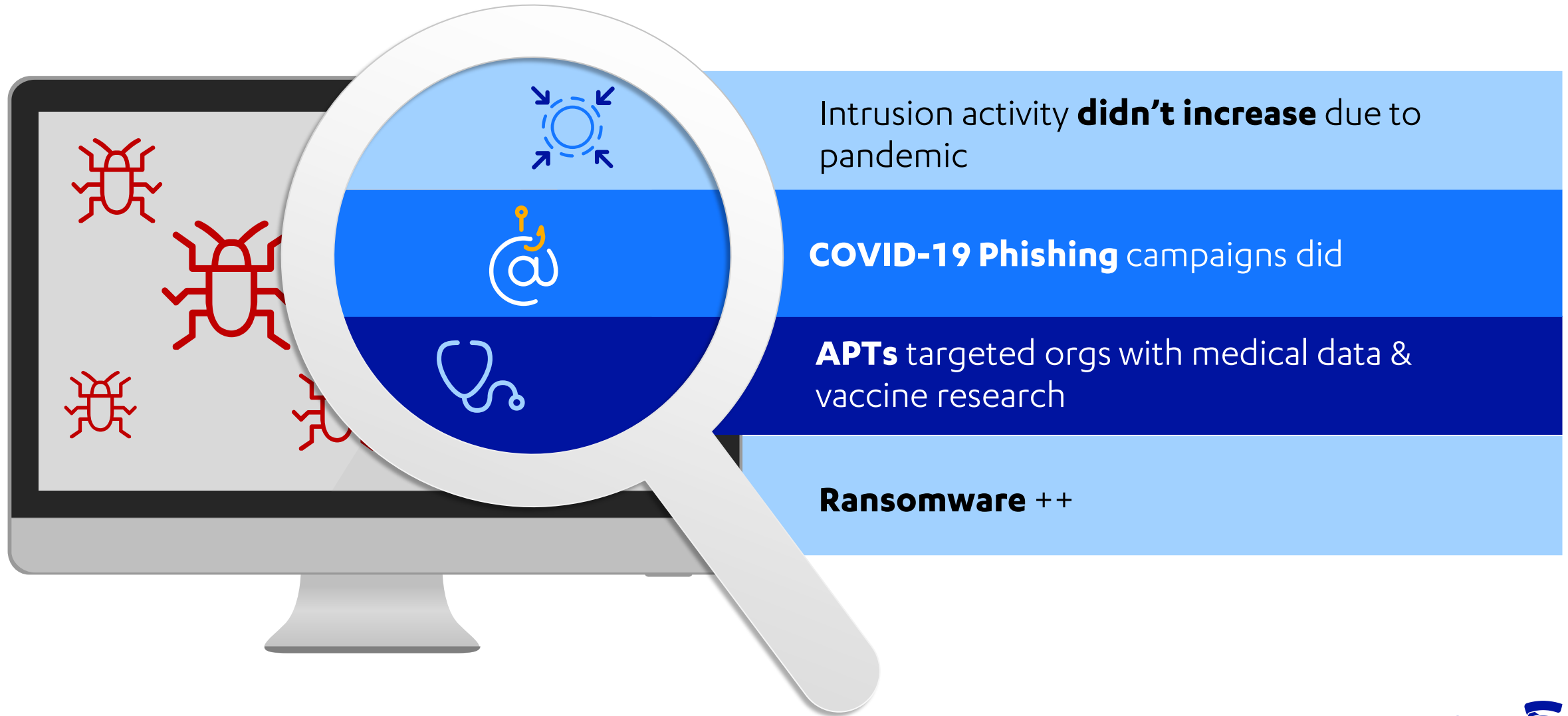


Critical
patching delays



IT teams focused on
continuing
operations,
not security

WHAT WE SAW: COVID VS. INCIDENT RESPONSE



Intrusion activity **didn't increase** due to pandemic

COVID-19 Phishing campaigns did

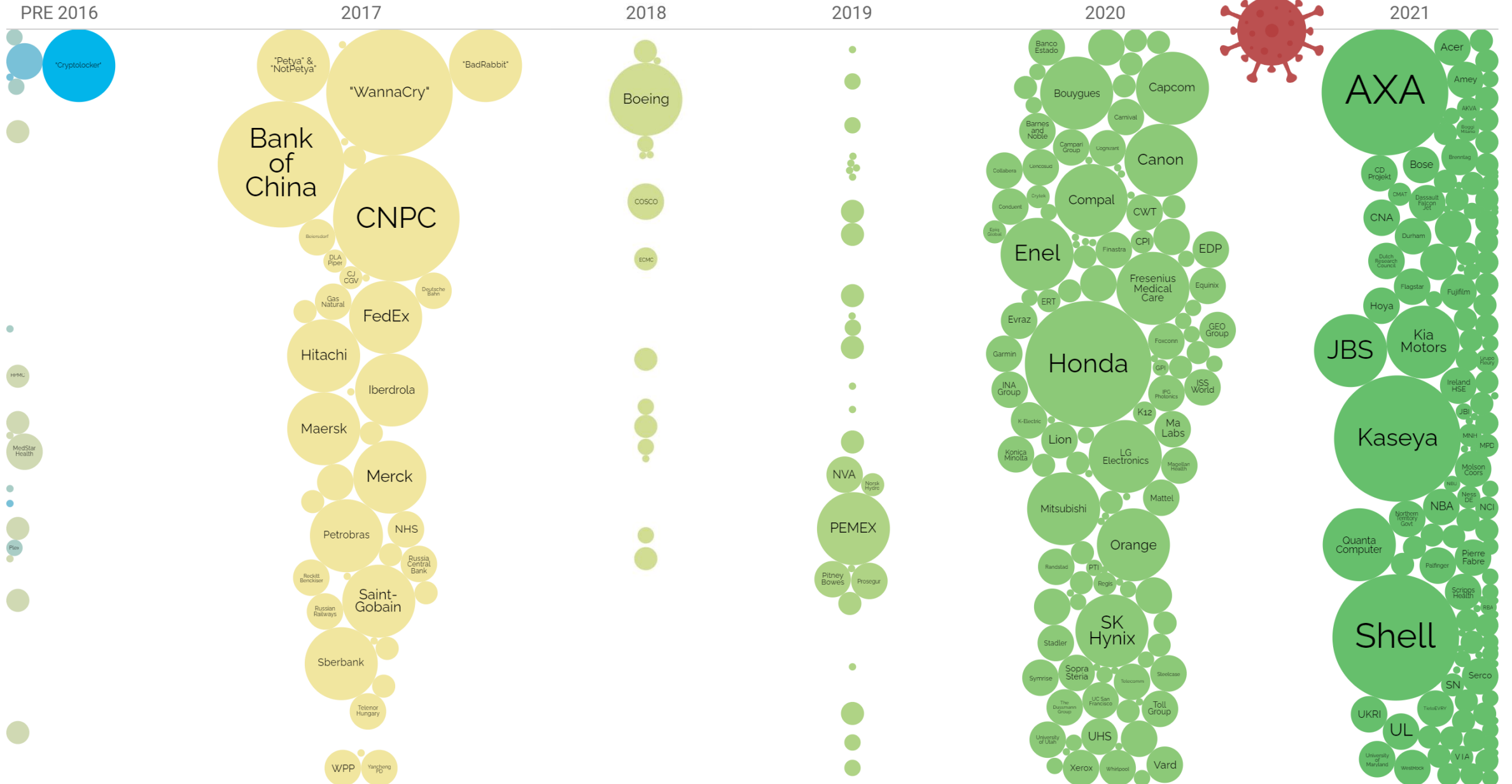
APTs targeted orgs with medical data & vaccine research

Ransomware ++

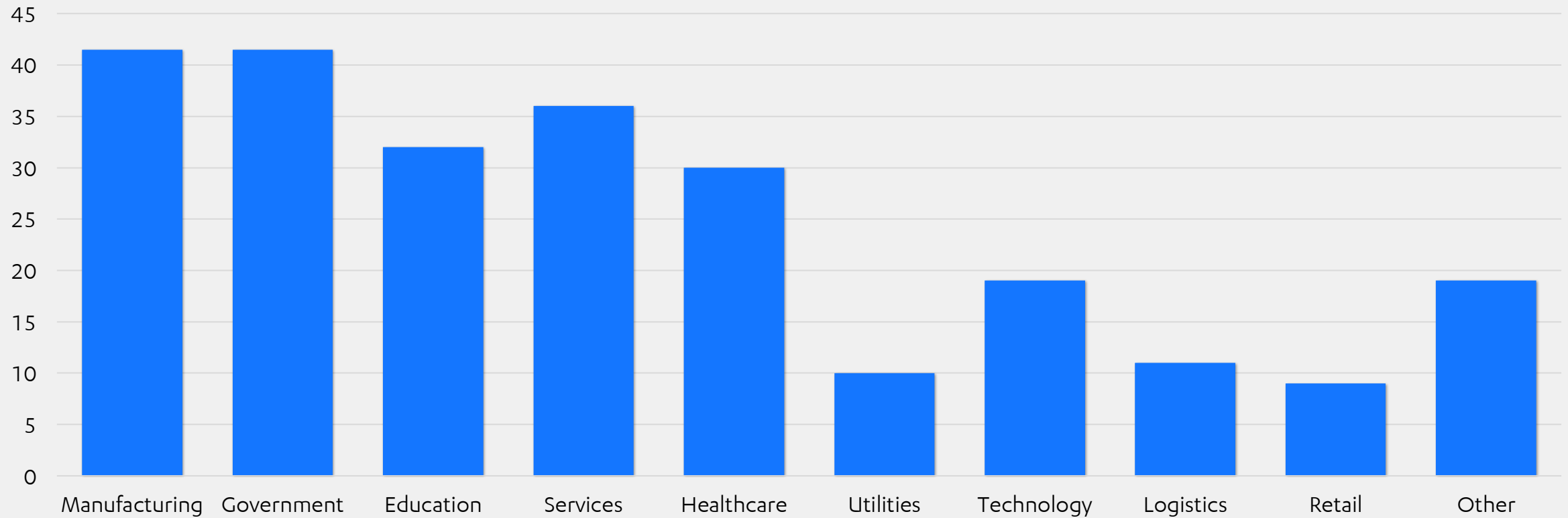
THE YEAR OF RANSOMWARE

RANSOMWARE ATTACKS

<https://informationisbeautiful.net/visualizations/ransomware-attacks/>

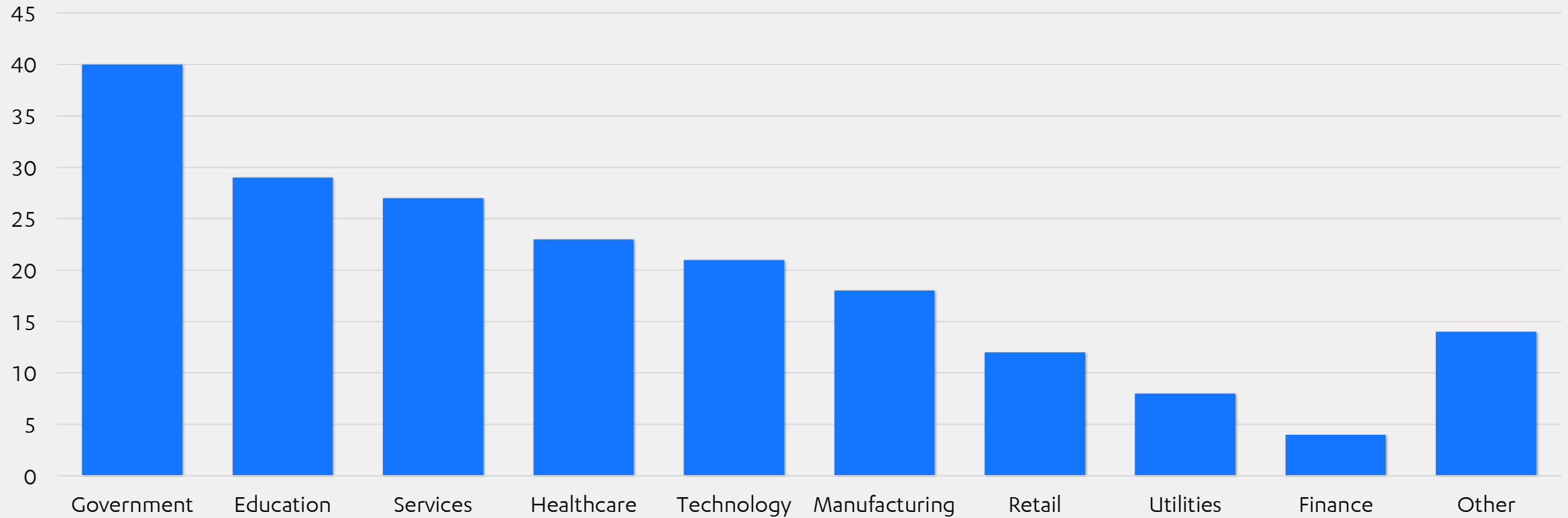


RANSOMWARE ATTACKS BY INDUSTRY 2020



Source: <https://www.blackfog.com/the-state-of-ransomware-in-2020/>

RANSOMWARE ATTACKS BY INDUSTRY 2021



Source: <https://www.blackfog.com/the-state-of-ransomware-in-2020/>

PANDEMIC IR CHALLENGES





HOW?

WHAT?

WHEN?



GOAL OF IR

IR APPROACHES

1 -> Live Threat



2 -> Post-Mortem



WITHOUT EARLY DETECTION, INCIDENT RESPONSE ALWAYS HAPPENS WHEN IT IS TOO LATE TO MINIMIZE THE IMPACT



IMPORTANT FACTORS

VISIBILITY THAT ENABLES EARLY DETECTION

- Where has the attacker been?
- Where are they now?

RESPONSE AT SCALE

- How do we collect data from the environment?
- How can we stop the attacker from reaching their objective?

THE STATE OF IR PRE-PANDEMIC

IR was already mostly remote



EDR technology enables rapid response and faster recovery



Traditional IR = inefficient & costly



THE BIGGEST CHALLENGES THE PANDEMIC BROUGHT TO ORGANISATIONS

- Communication in crisis
- Deploying EDR remotely
- Accessing the right data
- Recovery suffered



HSE spent nearly €700,000 setting up 'war room' after ransomware attack

Details of the spending have emerged following the publication of contract award notices by the health authority

Colonial Pipeline confirms it paid \$4.4m ransom to hacker gang after attack

The company's CEO authorized the payment as a means to restart the pipeline's systems quickly and safely

"Once they received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. **The tool was so slow that the company continued using its own backups to help restore the system,**" the story claimed, without naming a source.


London Borough of Hackney Struggles With Recovery Months After Ransomware Attack

Some ransomware victims deal with IT problems and backlogged work for long periods after an attack

RANSOMWARE IN FINANCIAL SERVICES

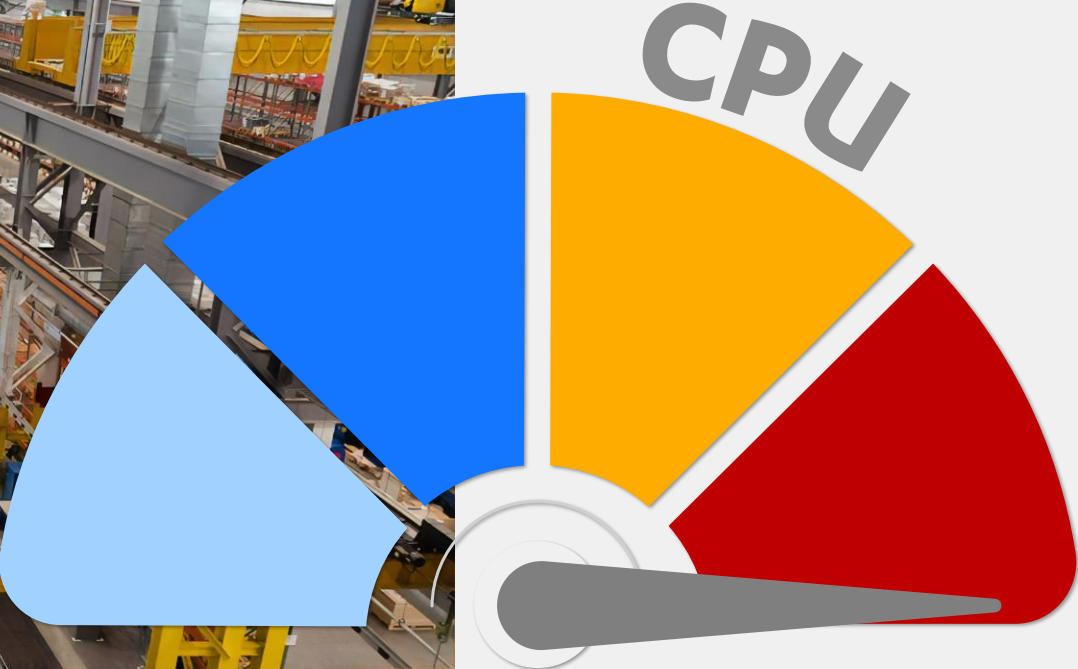
“The average bill for rectifying a ransomware attack in the financial services sector, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more, was US\$2.10 million.” – State of Ransomware in Financial Services 2021 Report,

Sophos

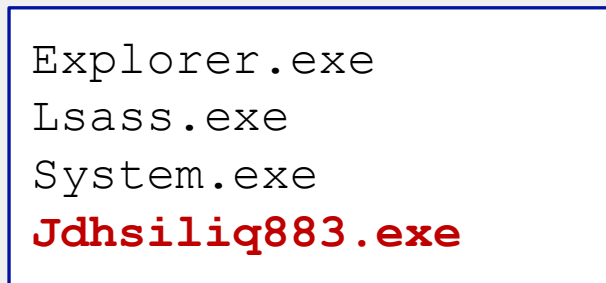
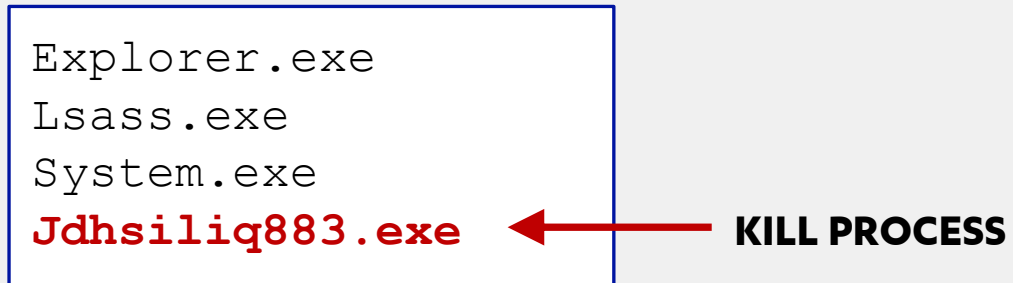


CASE STUDY: RANSOMWARE WHILE IN NATIONAL LOCKDOWN

SOMETHING IS NOT QUITE RIGHT



A CLOSER LOOK



AV Alert: Password Stealer

ITS SPREADING RAPIDLY

lockbit-decryptor.com/?9 4

YOUR FILES ARE ENCRYPTED BY LOCKBIT

What happend?

Many of your documents, databases, videos and other important files are no longer accessible because they have ben encrypted. Maybe you are busy locking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

THE RESPONSE





THE AFTERMATH

- Backups gone
- Domain had to be rebuilt from scratch, followed by the production servers
- Staff couldn't work until their devices were cleaned and rejoined to the domain
- Around 3 months to restore operations

HOW TO PREPARE



DEFINE & TEST YOUR PROCESSES



What could happen?

For every primary eventuality, **define & test the process**

Start simple: “A remote worker’s host has been compromised”.

“Our core communication system has gone down”

Business continuity & Disaster recovery

FOCUS ON THE PEOPLE

- **Educate** staff
- Make sure they know how to **report an incident** & what to look out for
- Provide **relevant** guidance on how to stay secure in a remote environment



WEAPONIZE YOUR TECHNOLOGY

- Increase your **visibility** and your **reach**
- Aggregate important **log data**
- Use **cloud technology** effectively



HOMework

1. Do you have **MFA** enabled?
2. Do you have **firewall logs** dating back at least **60 days**?
3. If you had an insider threat, could you stop them using the tech you already have?
4. Could ransomware affect your **backup servers**?
5. How will you **communicate** with your team in a **P1 incident**?
6. Could an IR team **remotely gather key evidence** from 100 hosts in your environment?
7. Could your infrastructure team **remotely remediate** a serious threat on your crown jewel servers?



F-Secure®