2024 Asia-Pacific Community Meeting

Case Study of a Card Data Breach Within A Ransomware Attack

PCI Security Standards Council

Thursday 21st of November 2024

PCI Security Standards Council

John Rundell

Managing Director Stratica
Core PFI and QSA

STRATICA®
ASIA LIMITED
IT & CYBER SECURITY | GOVERNANCE | RISK

Case Study of a Card Data Breach Within a Ransomware Attack

Outline of what I will cover

- What occurred
- Timeline
- What went wrong and why
- Lessons learnt
- Cyber insurance cover what's in and ransom cover YES or NO?
- Links to further information

PCI Security Standards Council®

Outline of What Occurred

- Business a subsidiary of listed Australian public company
  - medical pathology services holding over 11 million records
- What happened – A ransomware attack on 25 February 2022
  - All medical data encrypted, and ransom posted to computers.
  - Ransom $2M in bitcoins - but ignored making contact
- "Who ya gonna call?"– "Ghostbusters" a QSA used as Incident Responder.
- Company recovers all encrypted data from backups and Ghostbusters succeed
- Incident Responder (Ghostbusters) advises no data taken or credit card data impacted.
- Cyber insurer notified and law firm engaged. But no PFI called in!!
- Business gets going again and recovered data loaded to new servers.
- All infected servers wiped, and no images kept

BUT…Client data found on dark web 3 months later by ASD

Example only not actual

PCI Security Standards Council

Incident Response – Day One First 24 hours

Source: Collated from Findings of “ghostbusters” engaged QSA and Incident Responder

PCI Security Standards Council

Incident Response – Week one.
26 February to 1 March 2022 (and a bit more)

Source Findings of “ghostbusters” QSA and
Incident Responder

Root Cause Analysis

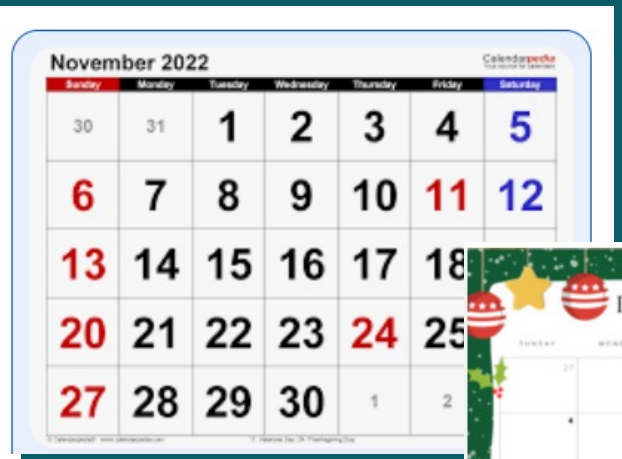
CONTROL FAILURES IDENTIFIED
- Security Email controls in MS365
- Limited Logs
- Webroot Antivirus
- Poor Vendor Management

What we know so far:

A doctor’s PC was infected and TSsel.exe was executed. Ttsel.exe executed in 2 parts. First it spread worm-like across the network and added attribute .quantum to all readable files. It then ran an execution to encrypt all .quantum files. The PC’s with Symantec, with no exceptions, detected the executable and quarantined it. Any PCs with Windows defender also quarantined the executable. Any machines with Webroot were vulnerable.

It is assumed that the Firewall (Firepower) IPS was not able to prevent the infection as the exploit was either delivered through a macro or email.

March 2022 to December 2022



Redacted letter to business

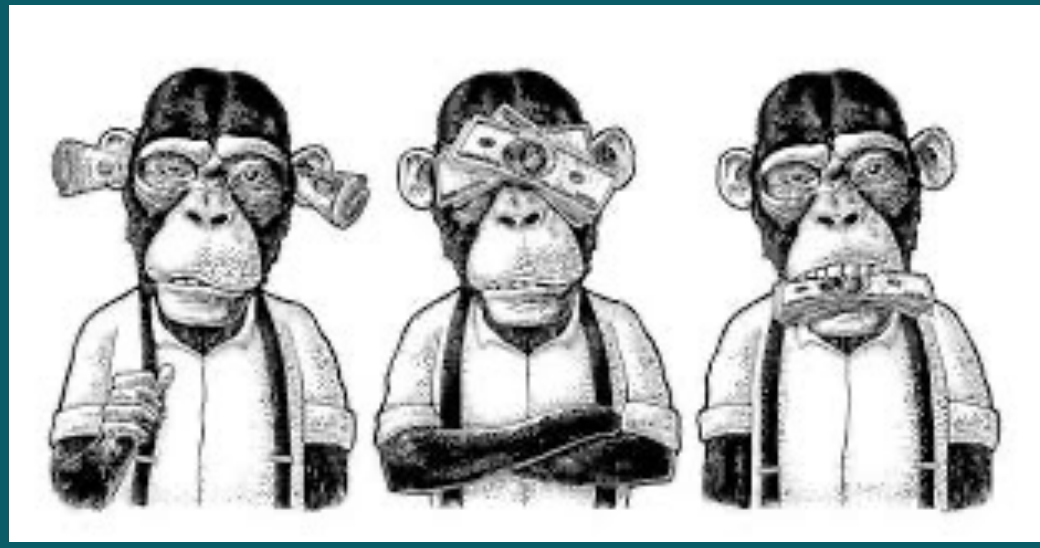
- Multiple contact from ASD AC ignored or not believed?
- 27 October 2022 Company announces data breach to Australian stock exchange
- SHARE PRICE FALLS 50%..... BRAND DAMAGE DONE
- 10 November 2022 _Payment Gateway writes to company and advises card brands of breach. Bank silent on breach

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

PCI Security Standards Council

AT LAST - 23 December 2022 Stratica a PFI engaged “UNDER LEGAL PRIVILEGE”

So, what did we find? - No forensic evidence Not PCI DSS compliant



- Only provided Ghostbusters Post Incident Review report and Incident Summary Report. Nothing more!
- Ghostbusters did NOT keep any of the logs or analysis.
- All infected servers and PCs had been wiped.
- No copy of the malicious code still available.
- Nothing to see here!
- A cover up from start to finish? Not really….An Incident responder is not a Forensic investigator understanding evidence preservation
- We learnt how hard it is to work under legal privilege!
- Card brands cleared Stratica to become QSA to company.
- Parent company was not PCI DSS compliant, but
- Signed SAQs covering all businesses including one during breach and subsequent year claiming that PCI compliant
  (Another QSA firm assisted via the bank).

PCI Security Standards Council®

Cyber Insurance – How Does It Work for Data Breaches?

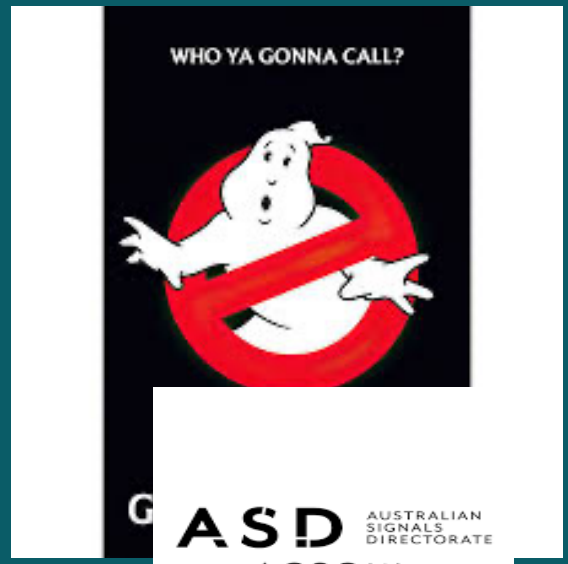
- How it works.
- What undertakings do you give?
  - PCI DSS security, etc.
    First up – Should you pay the ransom?
- What is covered?
  - Ransom cover and/or recovery costs
  - Can we recover from back-ups??
  - External support? Legal, PFI, incident response
- Are there Government restrictions on ransom payments?
- Ways around bans on ransom payments.

PCI Security Standards Council

Lessons Learnt and What Went Wrong

A lot was done wrong from the start!

- A QSA firm (codenamed Ghostbusters) as Incident Responder does not replace the need for a PFI.
- Whose role to contact impacted clients?
- Notifiable data breach? Who to notify and when?
- ASD engagement with private companies was and still is unclear.
- Ransomware Gang - to engage or not?
- Cyber insurance - what do you get?
- Whose role is it to engage a PFI?
- Whose advice should and can a company rely on?



ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Government
Office of the Australian Information Commissioner

PCI Security Standards Council

Thank You and Here Are Some Useful Links

Please ask me at the break on any specific questions

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

- Links: https://www.visa.com.au/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf
- https://www.asd.gov.au/
- https://www.cyber.gov.au/threats/types-threats/ransomware
- https://www.oaic.gov.au/__data/assets/pdf_file/0013/242050/Notifiable-data-breaches-report-January-to-June-2024.pdf
- https://www.Stratica.asia

PCI Security Standards Council

John Rundell
FCPA FCA FHKICPA QSA PCI Core FI

E: john.rundell@Stratica.com.au

Mobile: +61 419 568 506

Office: +61 3 9660 5700

https://www.Stratica.com.au

https://www.Stratica.asia

Payments Forensic Investigator

QSA across Austraia and in Singapre

With Core PFIs based in Melbourne, Sydney and soon Singapore


PCi
Security
Standards Council
®