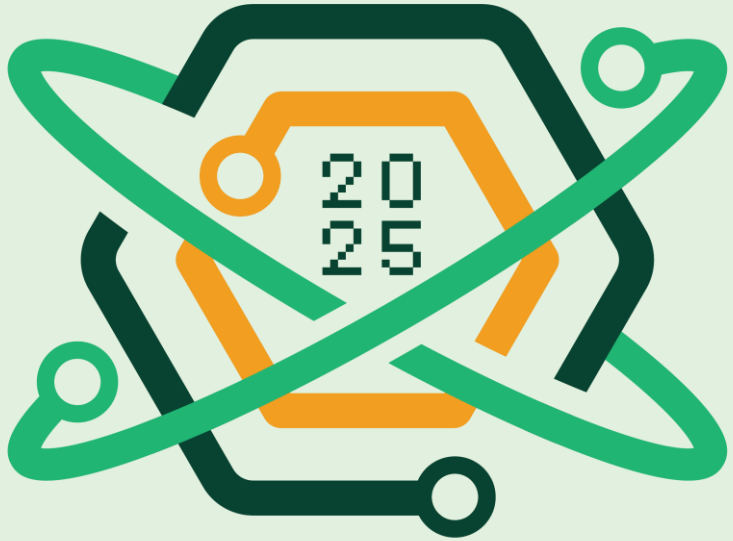


CYBER SYNC UP

COMBATTING CYBER CRIME

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

Welcome

—

KATRINA HICKSON

Head of Distribution
Emergence Insurance

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

Ransomware / Extortion Walkthrough

What happens when it happens

SLIDES REDACTED
TLP:RED - Not for circulation/distribution

JAMES FINLAY

Lead Director of
Incident Response, APJ
Coveware

When Cyber Hits the Fan

Real-life cyber incidents

LUKE FARDELL

Lead Cyber Analyst
Tokio Marine Kiln

NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

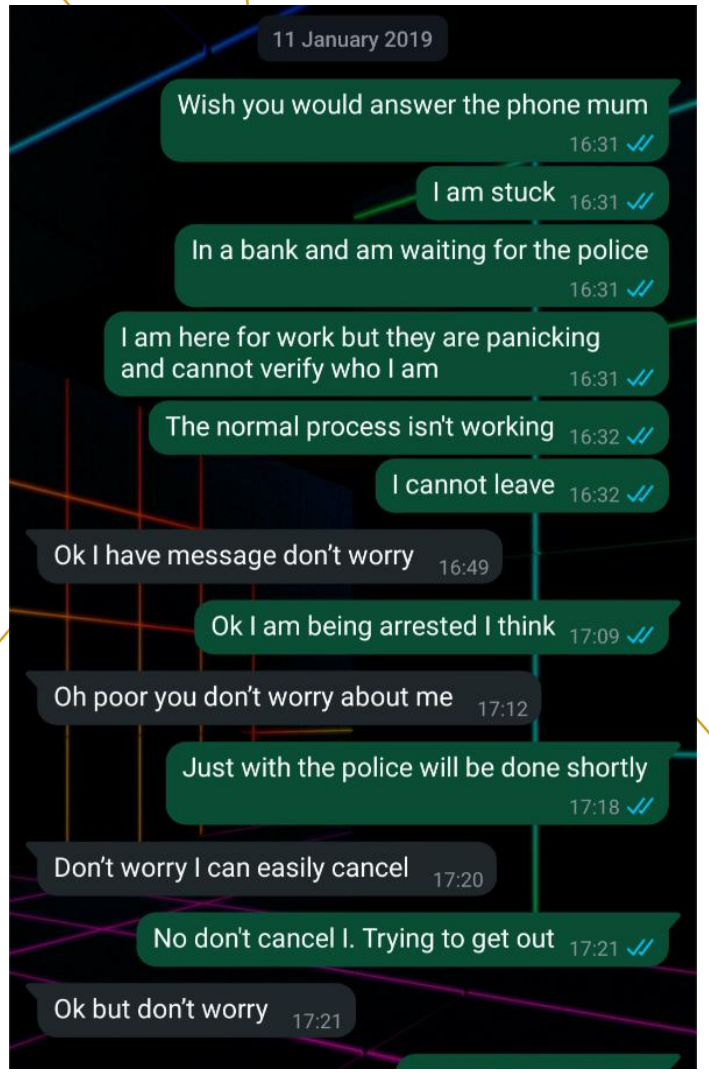
McGrathNicol

WK WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

When Cyber Hits The Fan

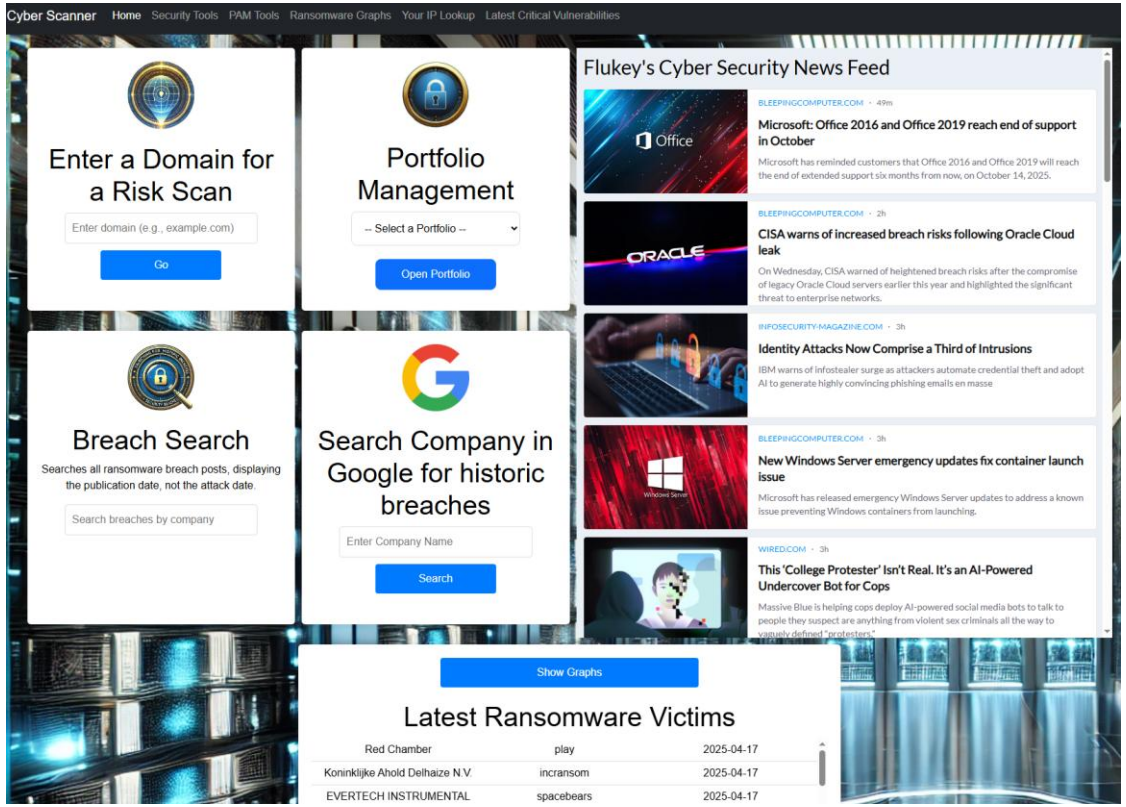
TOKIO MARINE KILN



CYBER SYNC UP 2025

Tokio Marine Kiln Role

- Lead Cyber Analyst
  - External attack surface scanning
  - Building tools
  - Helping on Complex Claims
  - Value Add services
  - Helping Group Companies
  - Bulk analysis of Coverholder portfolios



How I Ended Up Here

- It’s complicated

Interesting Cases

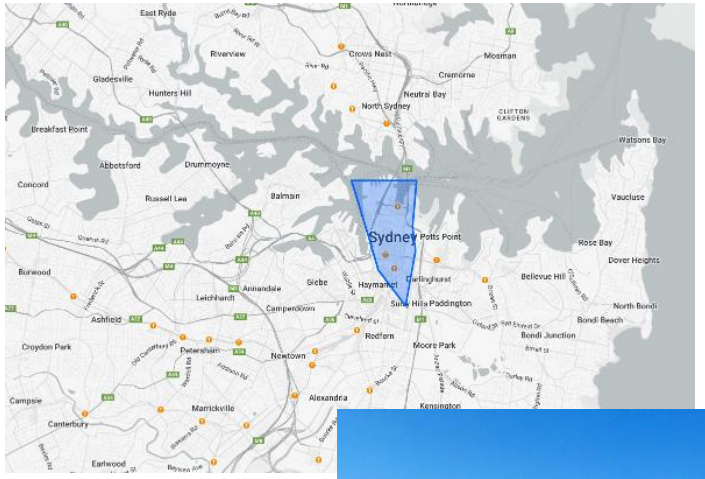
- The Salisbury Poisonings
  - Salisbury Hospital
  - Public Health England / Porton Down
  - Police Mobile phones

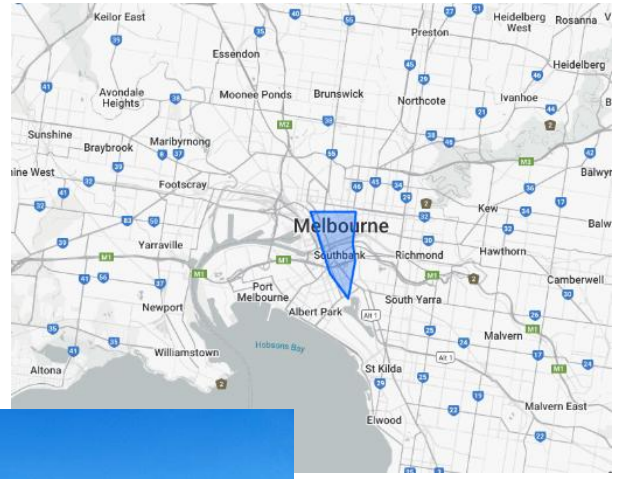
Prime Ministers Laptop

- Prime Minister Theresa May visits China in 2018

Gibraltar

- UK seizes Syria bound oil tanker off the coast of Gibraltar



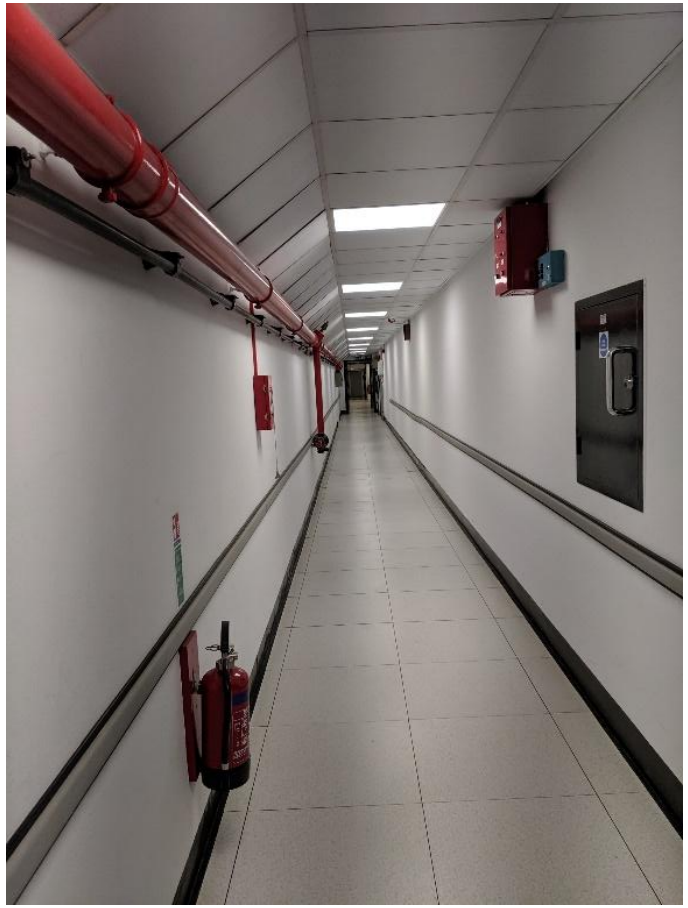


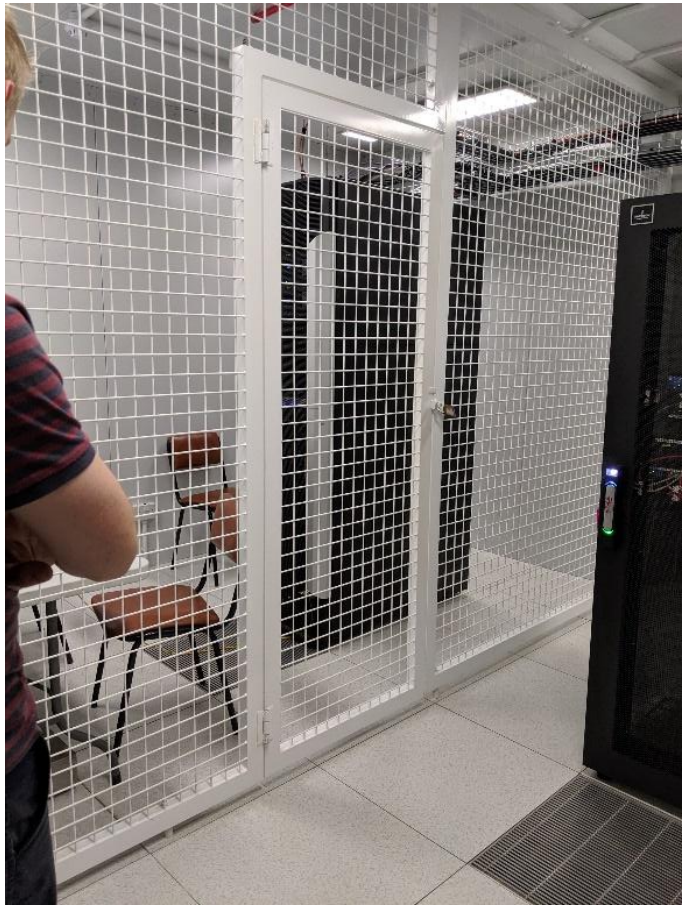
Iran fury as Royal Marines seize tanker suspected of carrying oil to Syria

Iran summons UK ambassador over incident off Gibraltar as tensions escalate over nuclear deal

An image issued by the Ministry of Defence of the supertanker Grace 1, believed to be carrying 2m barrels of crude oil. Photograph: MoD/PA

Gibraltar





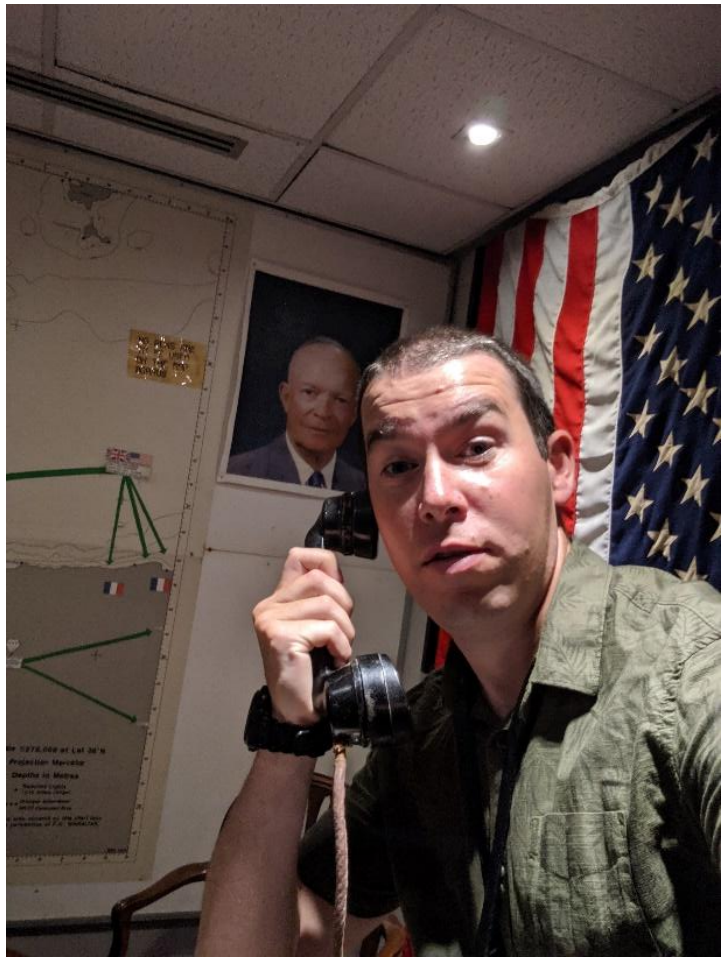

THIS ROOM WAS OCCUPIED BY
GENERAL DWIGHT EISENHOWER
COMMANDER IN CHIEF OF THE
ALLIED FORCES EMPLOYED IN
THE INVASION OF NORTH AFRICA
NOVEMBER 1942

Gibraltar


SHIP STATES
OWN SUB SURFACE FORCES


BIKINI ALERT STATE (USA)
RESPONSE FORCES
SHIP STATES
OWN SUB SURFACE FORCES

Gibraltar



Australia 2019

- Government wide cyber attack
- 5 eyes response
- Zero Day vulnerability
- ACSC lead

TOKIO MARINE KILN

Exclusive: Australia concluded China was behind hack on parliament, political parties – sources

By **Colin Packham**

September 16, 2019 4:50 AM GMT+1 · Updated 6 years ago

Aa

A man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration/Files Purchase Licensing Rights

CYBER SYNC UP

What it’s like working in DFIR

- Long hours
- No Weekends
- High stress
- Difficult conversations
- Often anger taken out on DFIR team
- Conflict with rebuild stream
- Costing difficult

But we love it

- The most rewarding part is the challenge

PANEL DISCUSSION

The Shifting Legal Landscape

Recent cases and updates

NICOLE GABRYK

Partner
HWL Ebsworth Lawyers

COLIN PAUSEY

Chief Operating Officer
Emergence Insurance

Threat Actors' Tactics, Techniques and Procedures

RICHARD GRAINGER

Head of Digital Forensics
Triskele Labs

NSB Cyber No Steps Backward

Triskele Labs

Hall&Wilcox smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH LAWYERS

Introduction

Richard Grainger

Head of Digital Forensics

- Studied Cyber Forensics at University.
- Worked in Law Enforcement for five years.
- Moved to internal DFIR teams.
- Moved to consulting.
- Leading a team of DFIR Analysts and Engineers responding to ransomware, business email compromise and other incidents.

DFIR at Triskele Labs

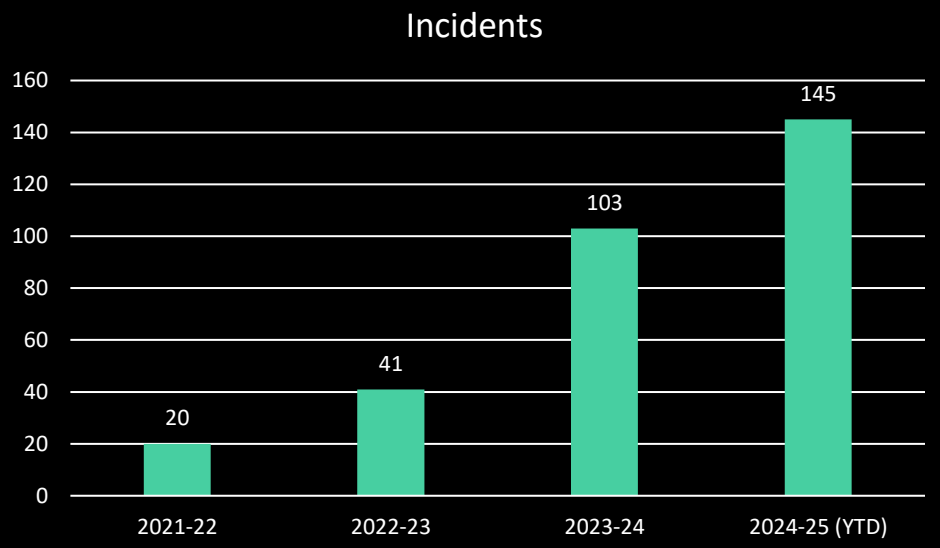
- 10 Years
- 5 Eyes Presence
- 100+ employees
- Australian based
- ISO27001
- ISO20000

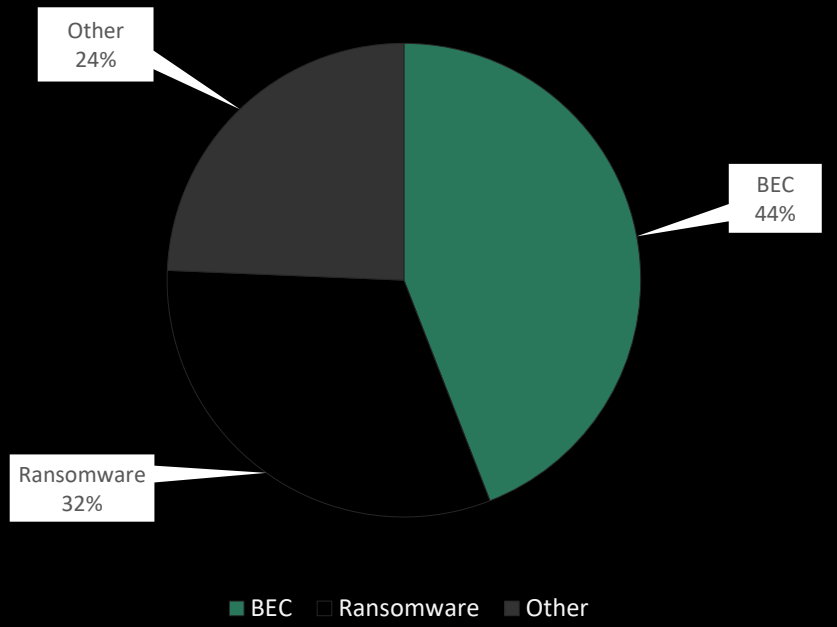
Threat Landscape

Setting the Scene

Incidents responded to

The Triskele Labs **Digital Forensics and Incident Response** team respond daily to incidents impacting small, medium and enterprise businesses.





Cyber security landscape

- Financially motivated Threat Actors targeting Australian organisations.
- State actors focused on critical infrastructure – data theft and disruption of business.
- Increase in media cover of cyber incidents.

Medibank hack: Russian sanctioned over Australia's worst data breach

23 January 2024

Optus: How a massive data breach has exposed Australia

Latitude Financial Scrambles to Contain Large Data Breach

Nissan Australia cyberattack claimed by Akira ransomware gang

Australian police arrest four BEC actors who stole $1.7 million

Western Sydney University discloses data breach, 7,500 'impacted individuals' notified

Western Sydney University (WSU) has revealed that its systems were breached by a threat actor, leading to student information being potentially exposed.

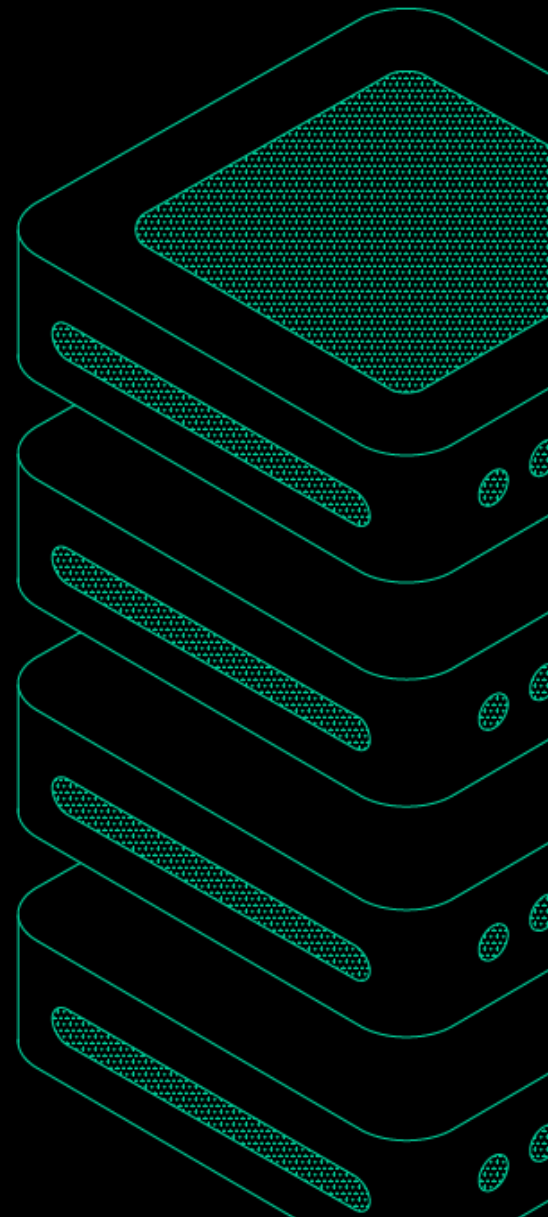
We've been ransomwared

What now?

If victim organisations have cyber insurance, call their incident response hotline.

Insurers maintain a panel of trusted vendors to help organisations respond to and recover from incidents.

- Digital Forensics and Incident Response
- Legal
- Crisis Communications
- Ransomware Negotiations



Digital Forensics and Incident Response

- Digital Forensics – examines electronic evidence to determine how an attack happened and what actions were performed.
- Incident Response – overarching process to prepare for, detect, contain and recover from an incident.

Threat Actor gains **unauthorised access** to one or more machines in a network.

Ransomware is executed, which encrypts (scrambles) **files**, making them **inaccessible**.

Only way to get the files back is to **pay the ransom** or have backups that can be restored from.

RANSOM NOTES

- Leave ransom notes on impacted machines.

  Print ransom notes across the organisation.

-- Qilin
Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data
We have downloaded compromising and sensitive data from your system/network.
Our group cooperates with the mass media.
If you refuse to communicate with us and we do not come to an agreement,
your data will be reviewed and published on our blog and on the media page
([redacted])

Blog links:
http://[redacted].onion
http://[redacted].onion

Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual
reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...

-- Warning
1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item
1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher
key. We encourage you to consider your decisions.

-- Recovery
1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials

Please note that communication with us is only possible via the website in
the Tor browser, which is specified in this note.

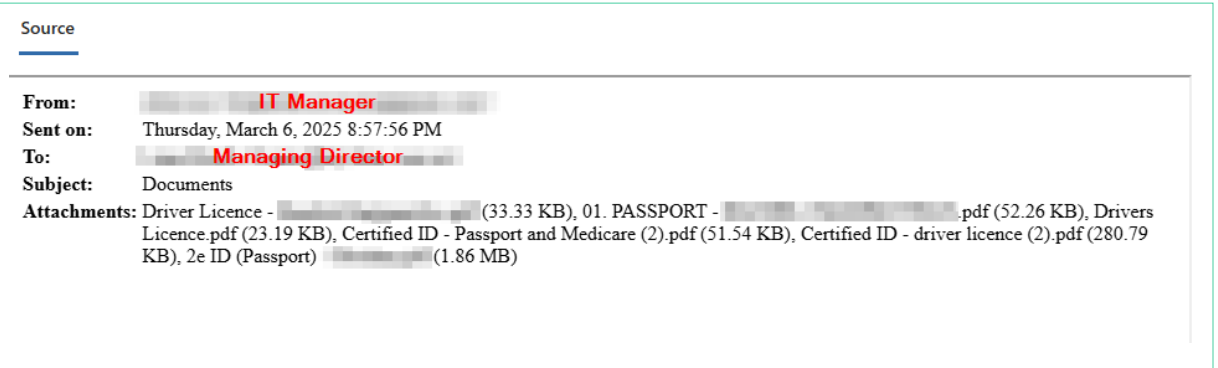
All other means of communication are not real and may be created by third
parties, if such were not provided in this note or on the website specified
in this note.

-- Credentials

Extension: [redacted]
Domain: [redacted]
login: [redacted]
password:[redacted]

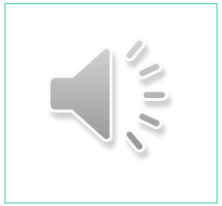
EMAILS

- Compromise internal mailboxes
- Send emails to staff



PHONE CALLS

- Gather C-Level contact details from the company website.
- Hire call centre services to call the victims and put pressure on them.

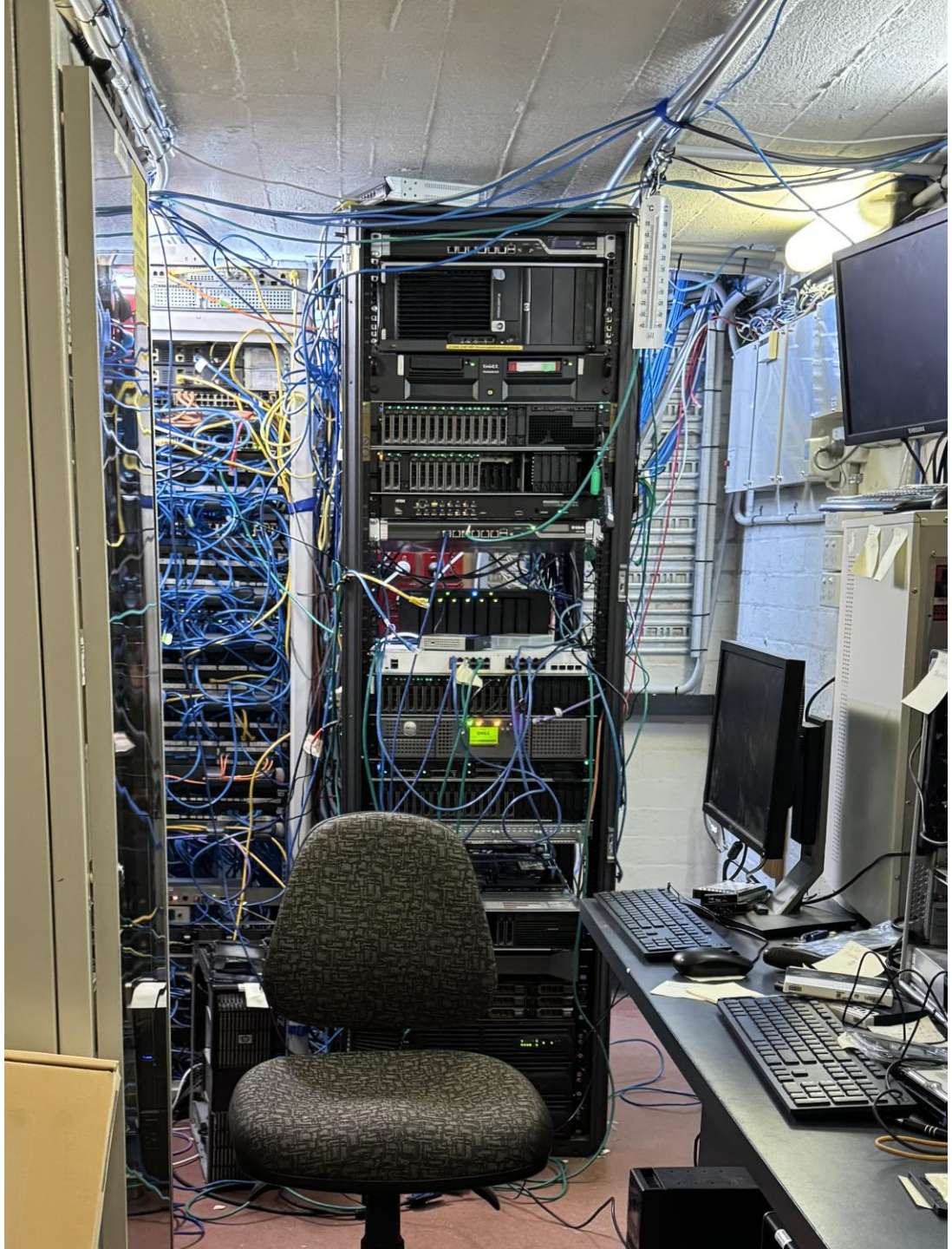


The Response

Let’s investigate

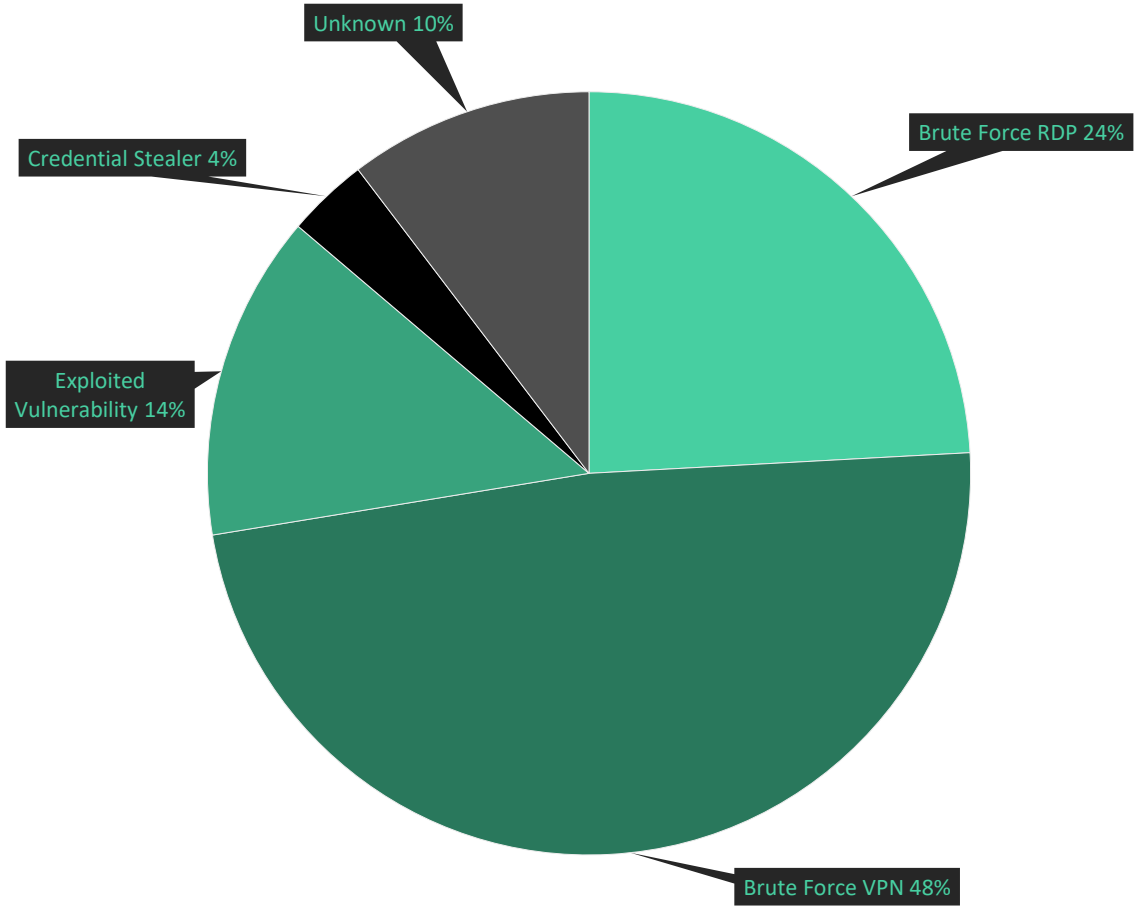
Initial Contact

- Scoping call with the client to understand what has happened.
- Deploy security and forensic tooling in the environment.
- Attend client site to assist with containment and evidence collection.

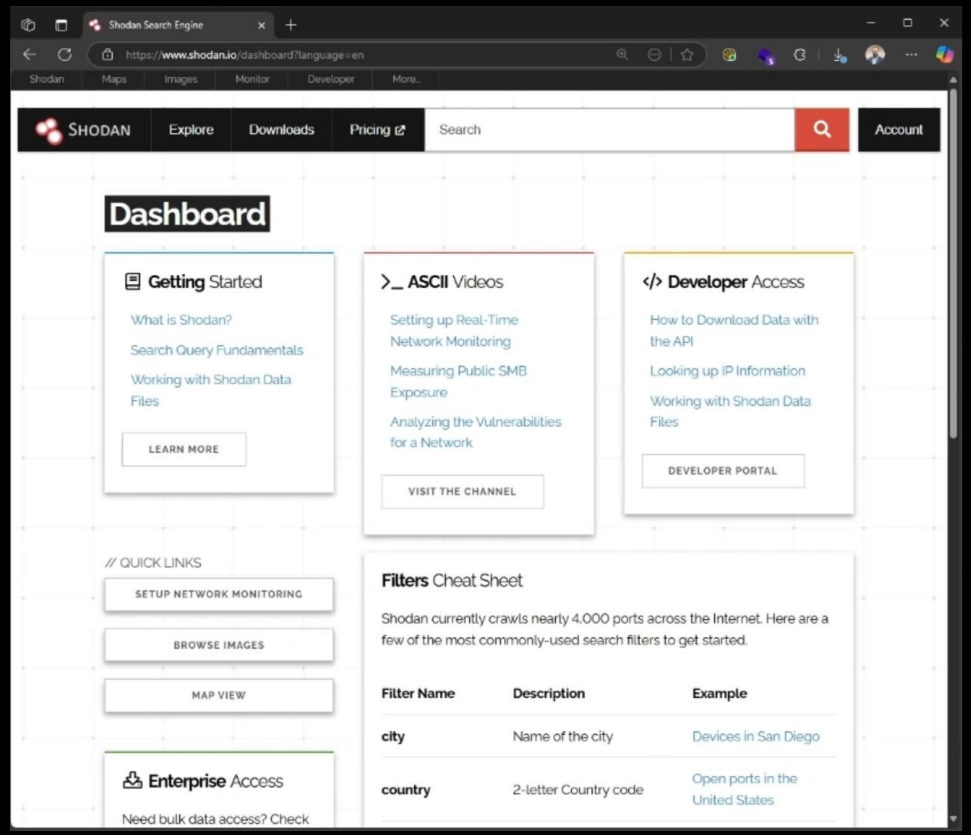


How did they get initial access?

- Misconfigurations on public facing infrastructure.
- Unpatched vulnerabilities.
- Information stealing malware to gain valid credentials.



Shodan Automation



- Shodan and Nuclei are powerful search engines that allows users to scan internet connected devices.
- Scan for devices susceptible to newly published critical vulnerabilities:
  - Citrix NetScaler
  - PaperCut
  - ScreenConnect
- Scan for devices susceptible to certain types of attacks:
  - VPN appliances without MFA
  - Remote Desktop Gateways

What data did they access or exfiltrate?

- Look for files or folders accessed by the Threat Actor.

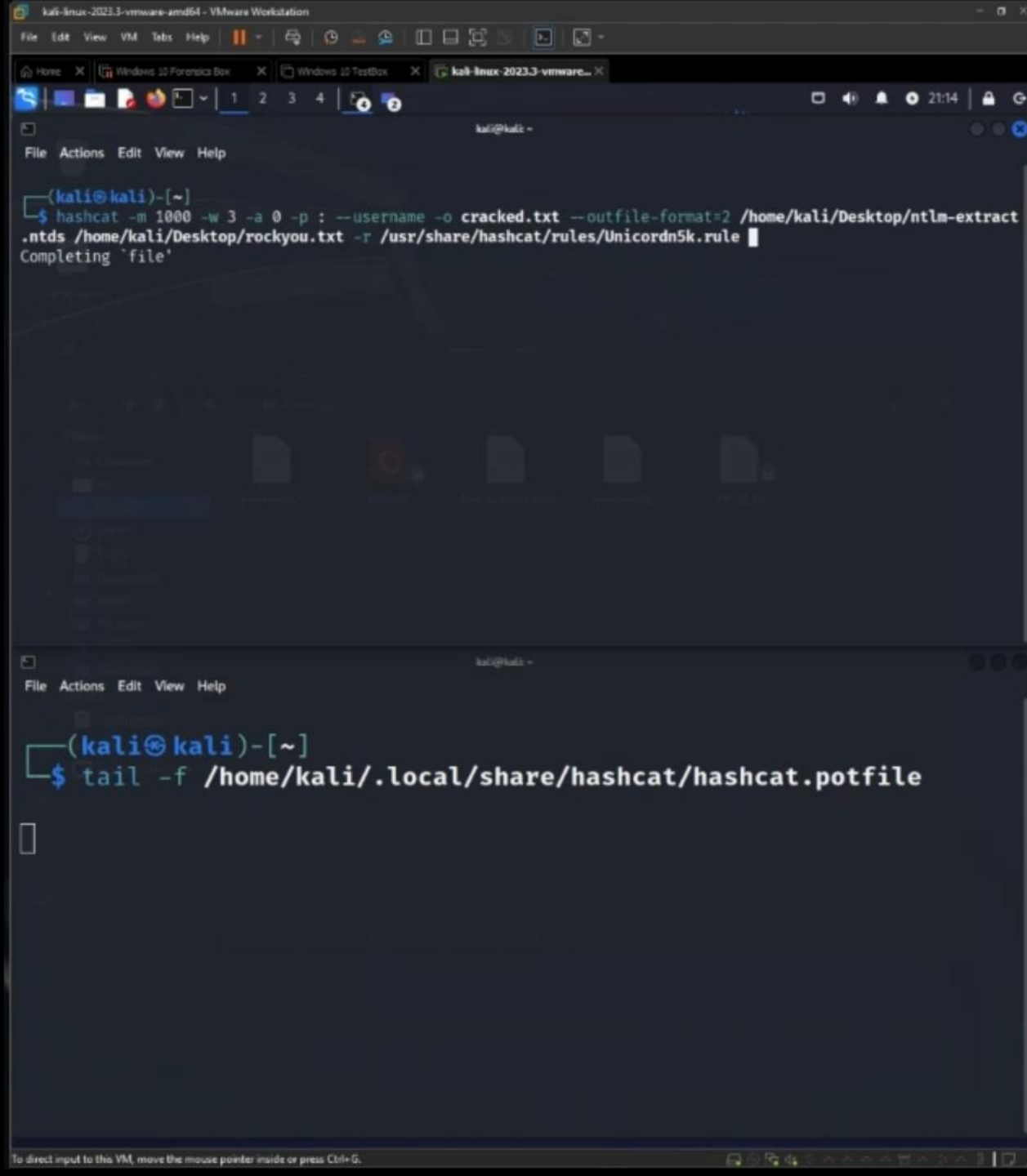
  Look for evidence of data staging.

- Find credentials to their infrastructure!

Path	First Interaction...
Control Panel:Programs and Features\	23/07/2024 12:53:48.000 PM
My Network Places:\ \Finance_Payroll\Payroll 24-25\	23/07/2024 1:09:24.000 PM
My Network Places:\ \Finance_Payroll\Payroll 24-25\	23/07/2024 1:09:27.000 PM
My Network Places: \d$\	23/07/2024 1:09:39.000 PM
My Network Places: \d$\	23/07/2024 1:09:43.000 PM
My Network Places:\ \Finance_INVOICES\Inv 24-25\	23/07/2024 1:10:13.000 PM
My Network Places:\ \Finance_INVOICES\	23/07/2024 1:10:48.000 PM
My Network Places:\ \hr\Personnel\	23/07/2024 1:11:30.000 PM
My Network Places:\ \hr\Personnel\	23/07/2024 1:11:41.000 PM
My Network Places:\ \c$\Deploy\	23/07/2024 1:11:53.000 PM
My Network Places:\ \c$\Deploy\	23/07/2024 1:11:56.000 PM
My Network Places:\ \c$\HR\Project Admin\	23/07/2024 1:12:22.000 PM
My Network Places:\ \c$\HR\Project Admin\	23/07/2024 1:12:26.000 PM
My Network Places:\ \c$\HR\Recruitment\Current Offers\	23/07/2024 1:12:42.000 PM
My Network Places:\ \c$\HR\Recruitment\Current Offers\	23/07/2024 1:12:47.000 PM
My Network Places:\ \c$\HR\Recruitment\Current Offers\ \	23/07/2024 1:12:49.000 PM
My Network Places:\ \c$\HR\Recruitment\Current Offers\ \	23/07/2024 1:13:09.000 PM

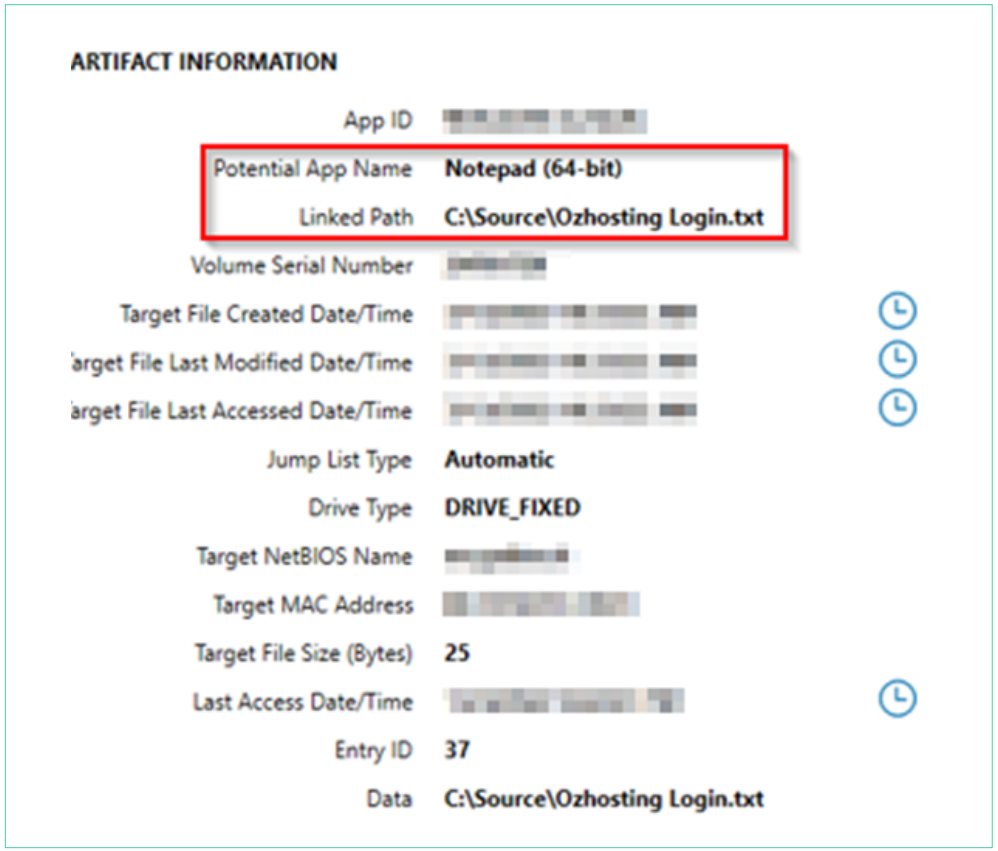
How did they get privileged access?

- Exploiting a vulnerability.
- Weak passwords – they can be easily cracked!



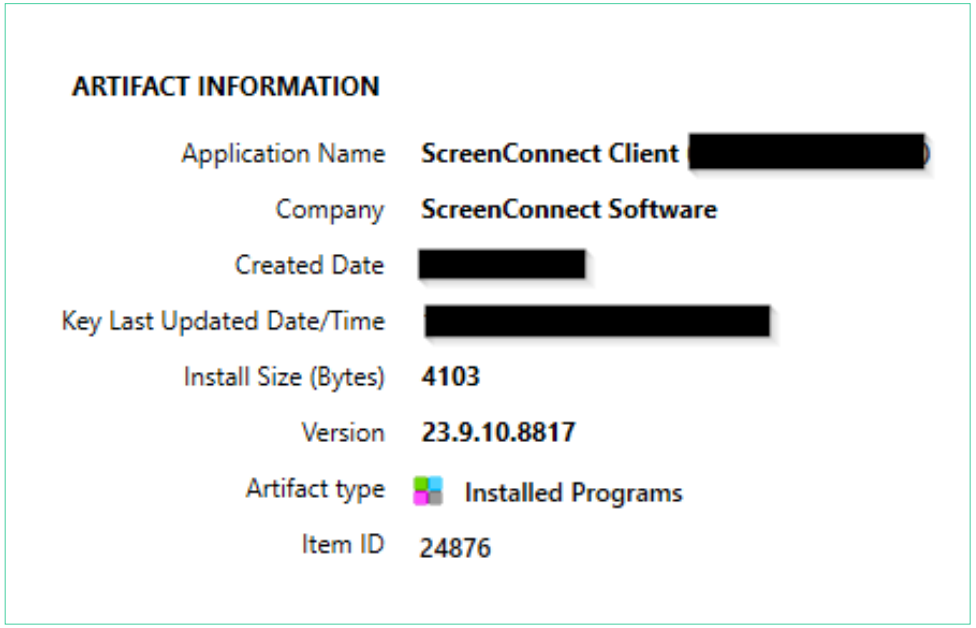
How did they destroy our backups?

- Sometimes a Threat Actor gets lucky, and finds credentials contained in plaintext files.
- Organisation was performing backups onto domain joined NAS, and cloud backups to OzHosting.
- Dumping of credentials using tools.
- MSP left username and password to OzHosting in a .txt file on a server.
- Organisation had to pay $100,000 USD ransom to obtain decryptor.



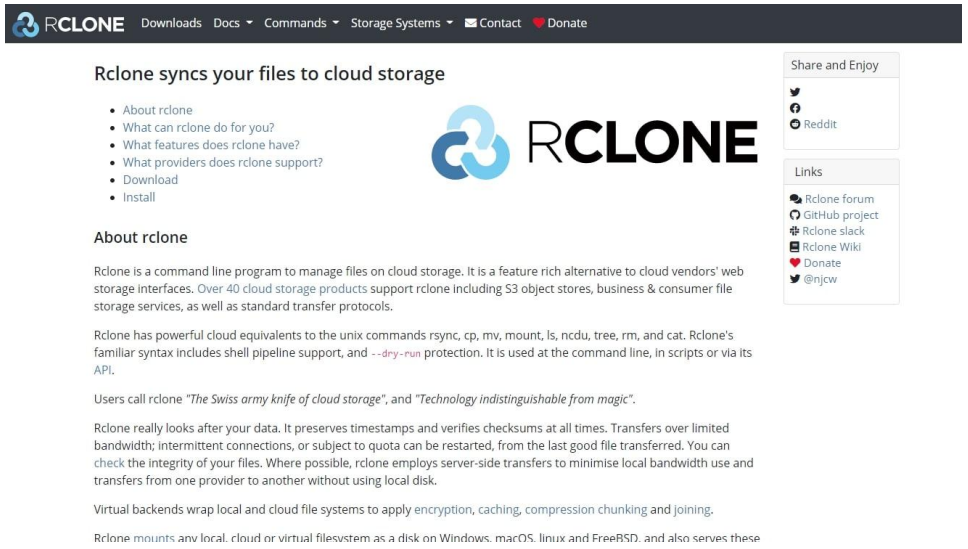
Are they still in our environment?

- Threat Actors will frequently install legitimate Remote Management and Monitoring (RMM) tools, which blend into the environment – AnyDesk, ScreenConnect, Atera, Level, Simplehelp, Teamviewer.
- In this case the Threat Actor stayed undetected in the environment for months as the same RMM was used legitimately by the MSP.



How did they steal our data?

- Rclone is command-line program to manage files on cloud storage.
- Threat Actors will exfiltrate data using various methods such as FTP, MEGA, GoFile.
- Throttled during the day, full speed overnight to avoid detection.



How did they encrypt our data?

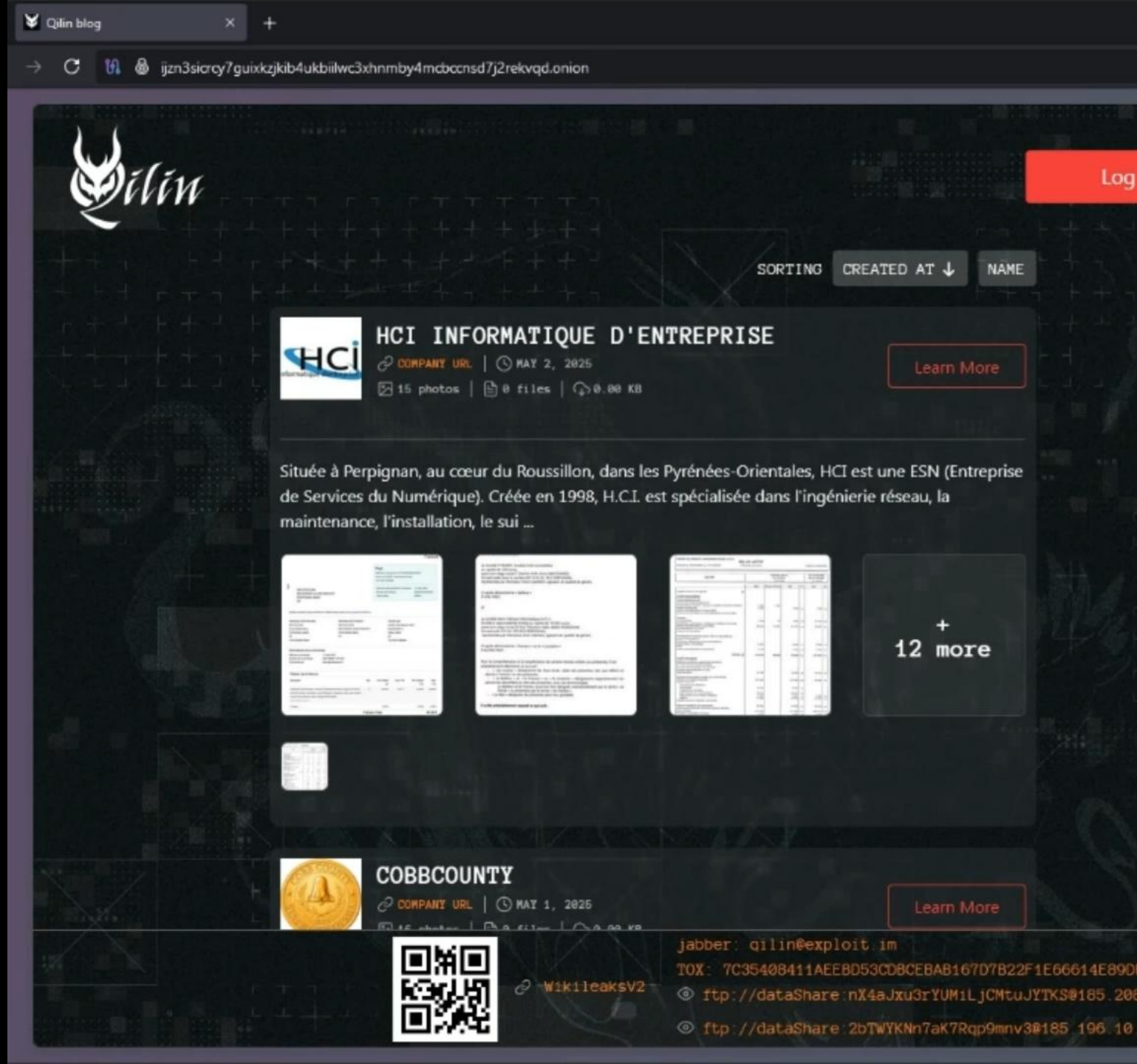
- Ransomware binary deployed across the environment.
- Threat Actor created a Group Policy Object to copy the binary to each domain joined host and then execute it.

The Aftermath

Data

Data published on leak site

- Threat Actors maintain leak sites on the dark web.
- Publish victim organisation names and stolen data.



Notification to impacted individuals

- Understand what data has been impacted.
- Harm assessment.
- Notification to impacted individuals.

VINOMOFO

Hi Richard,

I am writing to provide you with some important information about a recent cyber security incident at Vinomofo.

Vinomofo experienced a cyber security incident where an unauthorised third party unlawfully accessed our database on a testing platform that is not linked to our live Vinomofo website.

We immediately engaged leading cyber security and forensic specialists (including IDCARE, Australia's national identity and cyber support service) to investigate the claim and took steps to further secure our IT environment and strengthen our systems.

We also reported the matter to the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC).

Our investigation established that customers' and members' information on our database on this testing platform was unlawfully accessed by a third party. **However, our cyber security and forensic specialists have assessed that the risk to our customers and members by this information being accessed is low.**

Vinomofo does not hold identity or financial data such as passports, drivers' licences or credit cards/bank details.

While no passwords, identity documents or financial information were accessed, the database includes other information about customers and members.

The information about you that was contained in the database that may have been accessed may include name, gender, date of birth, address, email address and phone number.

Recommendations

Tips for Brokers

Tips for Brokers

Patch internet-facing systems, fast.

Use stronger passwords and a password manager.

MFA, always.

AV is not EDR. Not all EDRs are equal.

Hold IT MSPs to account.

24x7x365 monitoring. Also, not all SOCs are equal.

THANK YOU

PANEL DISCUSSION

Dispatches from the Frontline

LUKE FARDELL

Lead Cyber Analyst
Tokio Marine Kiln

CRAIG MARTIN

Incident Response Manager
Triskele Labs

KIERAN DOYLE

Head of Cyber & Technology
Wotton + Kearney

PETER FURST

Head of Incident Response
Emergence Insurance

NSB Cyber
No Steps Backward

Triskele Labs

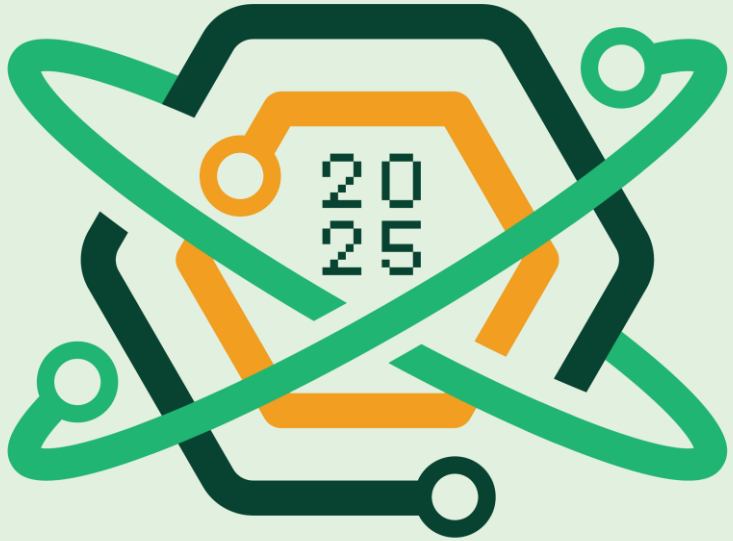
Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS

THANK YOU



NSB Cyber
No Steps Backward

Triskele Labs

Hall&Wilcox
smarter law

McGrathNicol

WOTTON KEARNEY

HWL EBSWORTH
LAWYERS