2013 - 2023 in Cyber

Why do I keep banging my head against a brick wall

Iain Dickson

Who the hell is this guy?

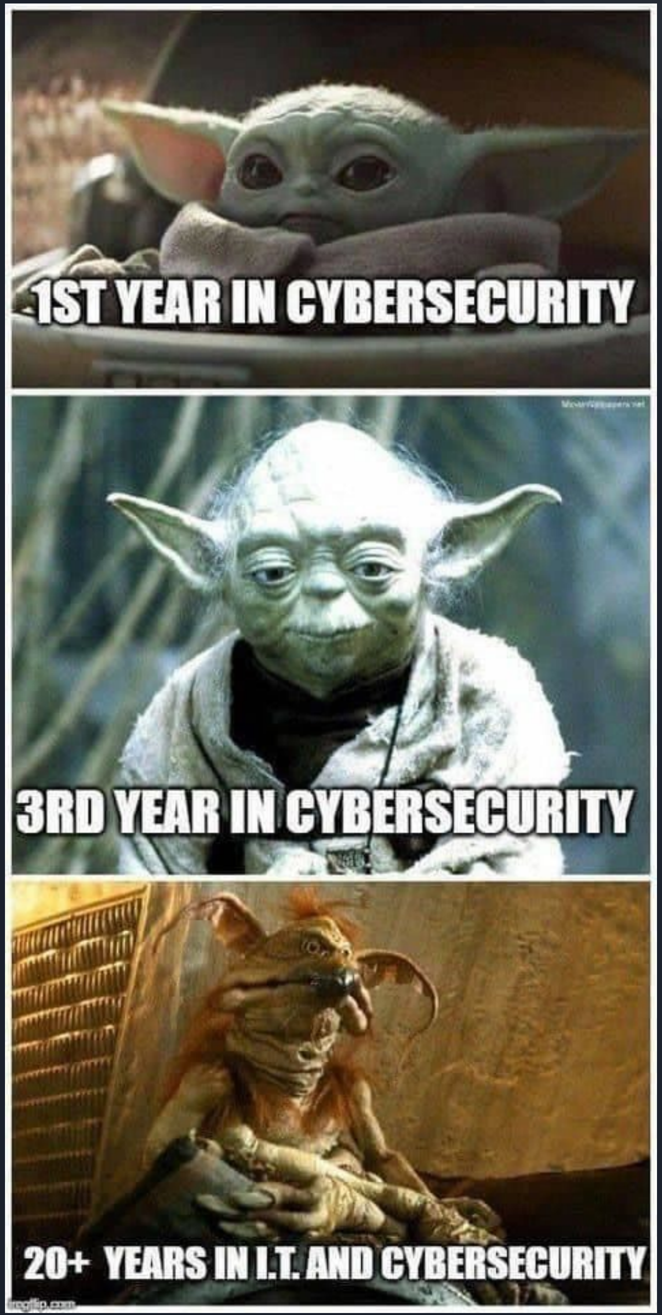
- 10 years in Cyber Security, 13 (inclusive) in IT

- Previous Positions
  - Cyber Security Researcher at AU DOD
  - Cyber Security Research Engineer at AU DOD
  - Assistant Director Cyber Threat Intelligence Technical Capability at AU DOD
  - Security Operations Centre Lead at Leidos Australia
  - Chief Cyber Architect at Leidos Australia

- Currently the Cyber Practice Manager for Leidos Australia, reporting up to the CTO.

- Founder for ComfyConAU

This presentation does not represent the views of my employer.


1ST YEAR IN CYBERSECURITY
3RD YEAR IN CYBERSECURITY
20+ YEARS IN I.T. AND CYBERSECURITY
imgflip.com

2013
The Mandiant APT 1 Report

MANDIANT®

APT1

Exposing One of China's Cyber Espionage Units

Threat, Vulnerability, and Risk

Threat

Any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals.

×

Vulnerability

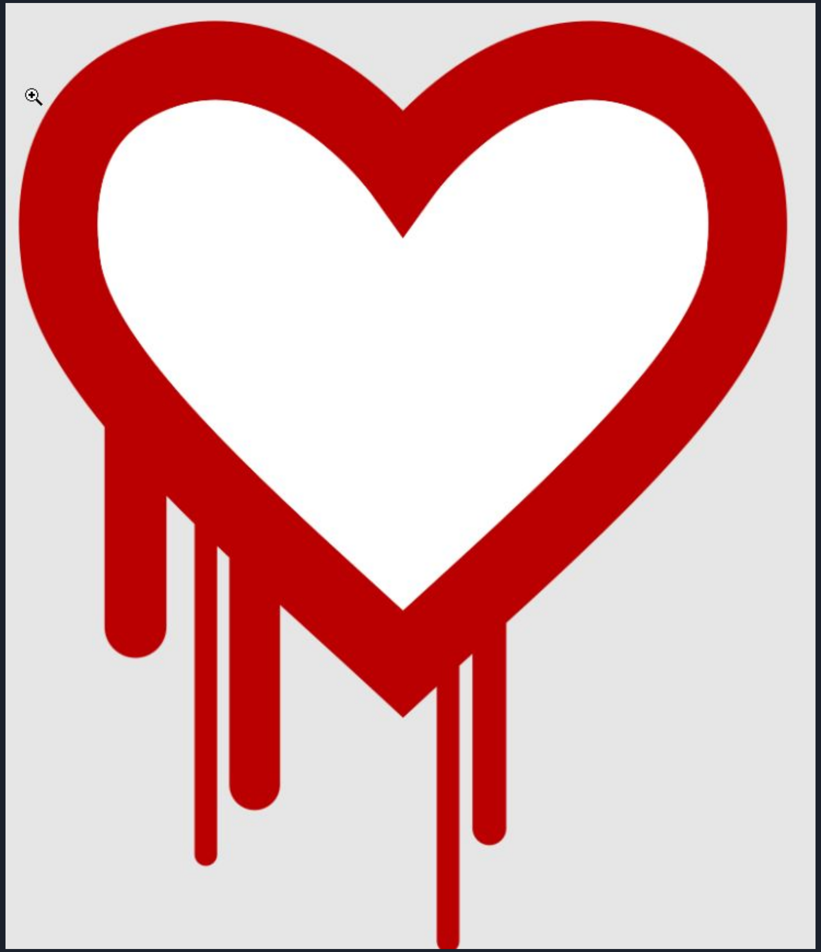
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered.

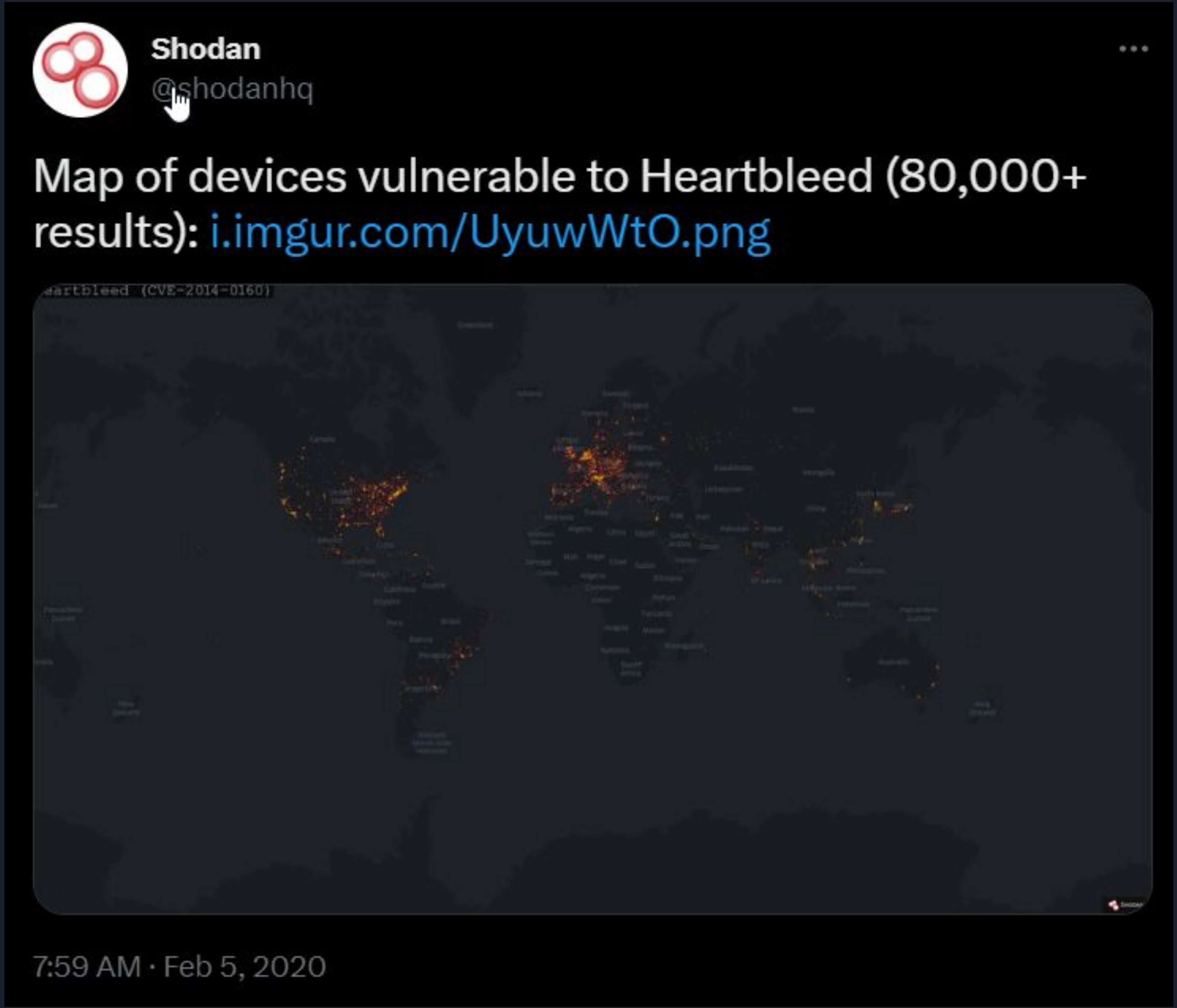
→

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

2014
Heartbleed



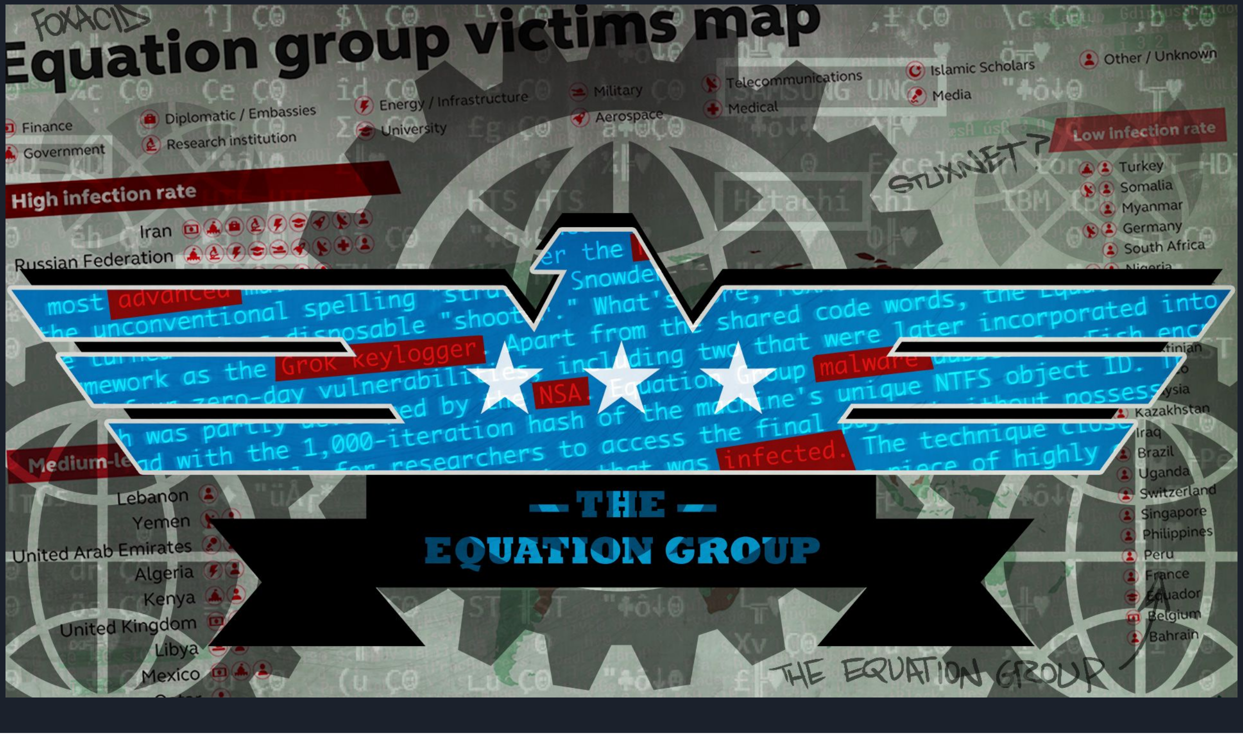


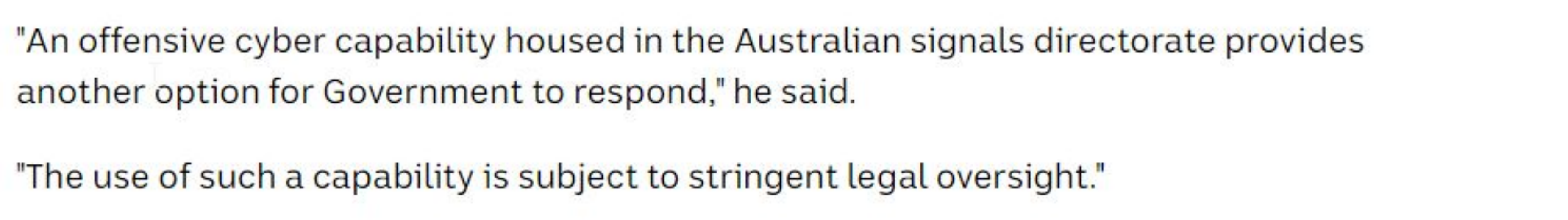
Shodan
@shodanhq

Map of devices vulnerable to Heartbleed (80,000+ results): i.imgur.com/UyuwWtO.png

7:59 AM · Feb 5, 2020

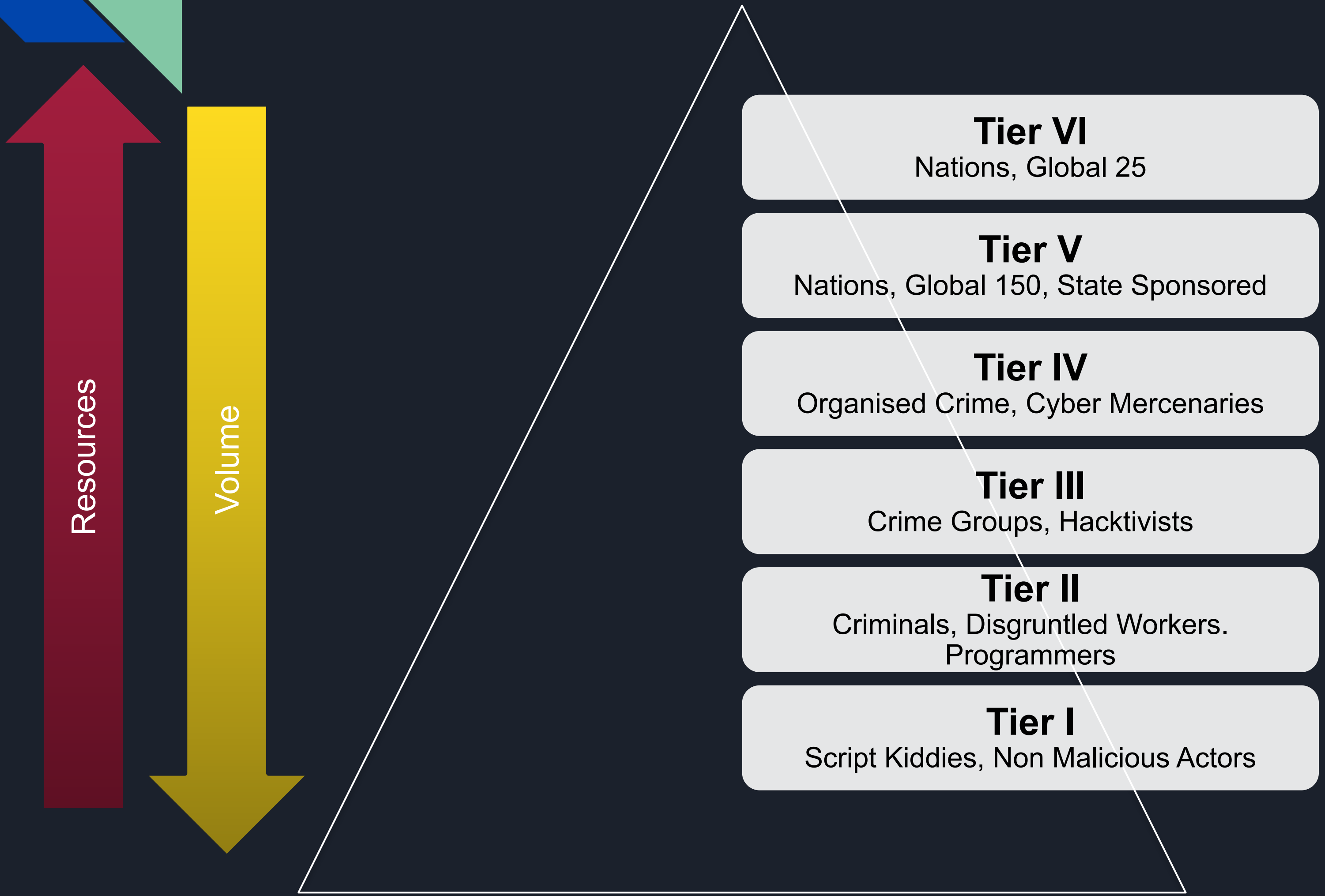
2016
Equation Group and ASD




"An offensive cyber capability housed in the Australian signals directorate provides another option for Government to respond," he said.

"The use of such a capability is subject to stringent legal oversight."

Threat Actor Tiers



Tier VI
Nations, Global 25

Tier V
Nations, Global 150, State Sponsored

Tier IV
Organised Crime, Cyber Mercenaries

Tier III
Crime Groups, Hacktivists

Tier II
Criminals, Disgruntled Workers. Programmers

Tier I
Script Kiddies, Non Malicious Actors

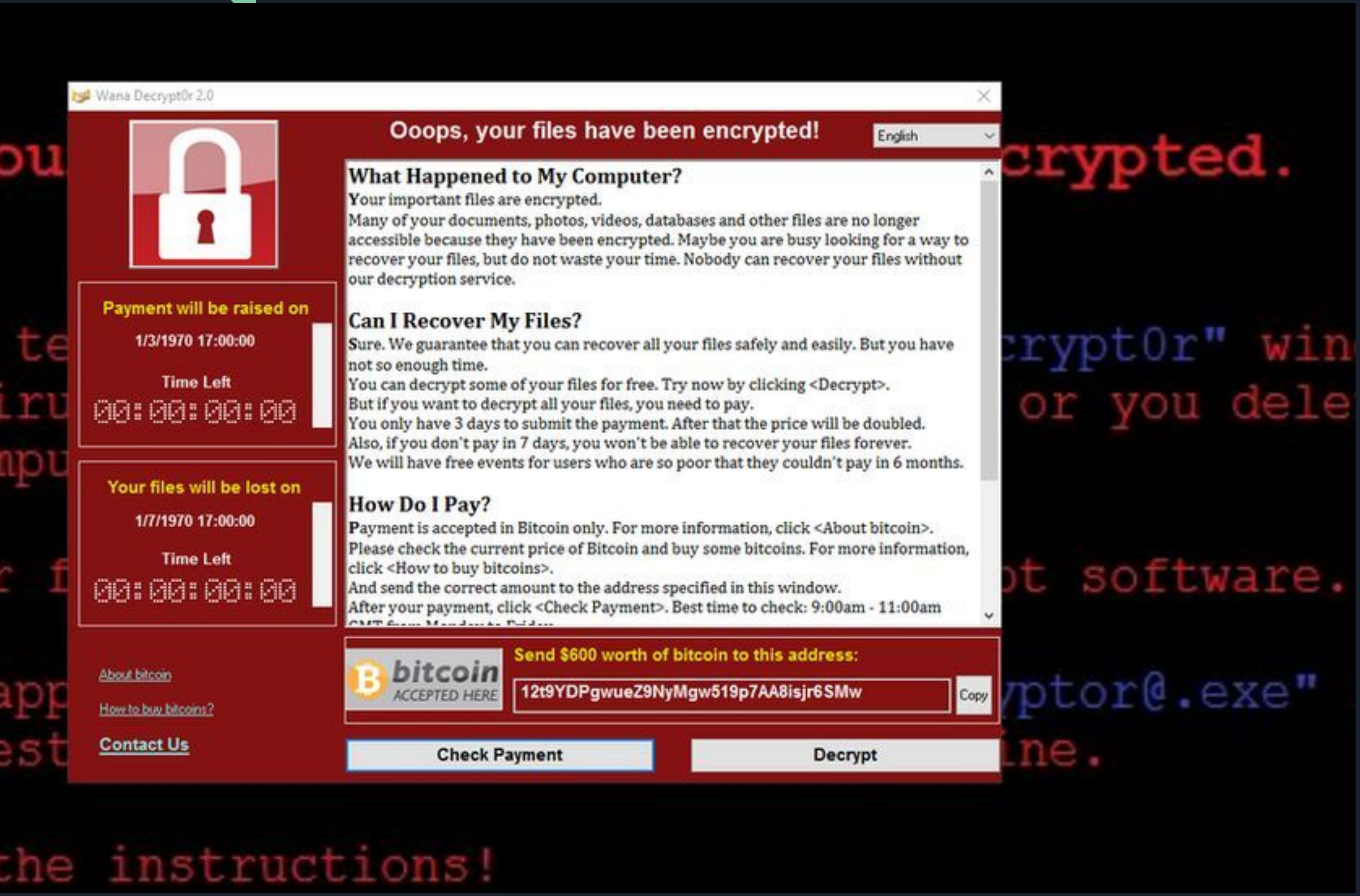
Creates Vulnerabilities using Full Spectrum

Discovers Unknown Vulnerabilities

Exploits pre-existing, known vulnerabilities

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

2017
Wannacry, NotPetya, X-Agent



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

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

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on

1/3/1970 17:00:00

Time Left

00:00:00:00

Your files will be lost on

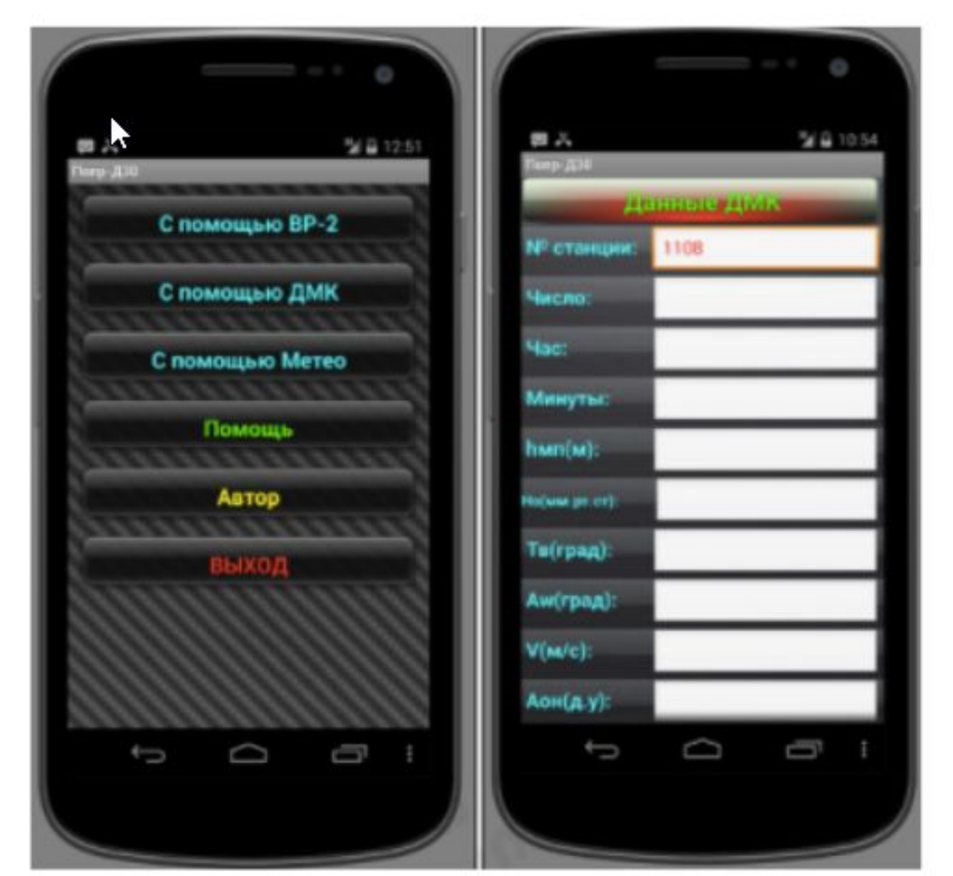
1/7/1970 17:00:00

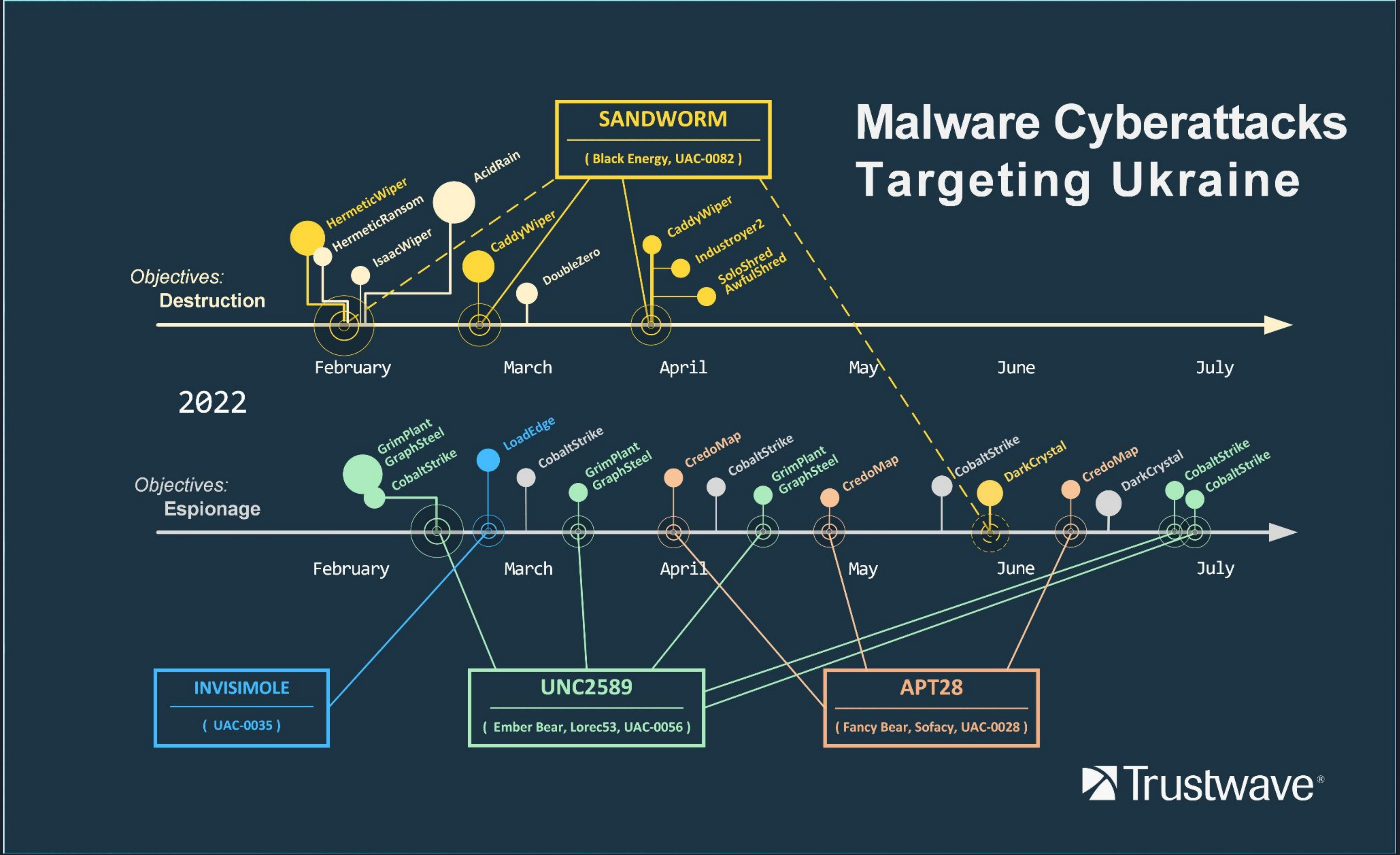
Time Left

00:00:00:00

Send $600 worth of bitcoin to this address:

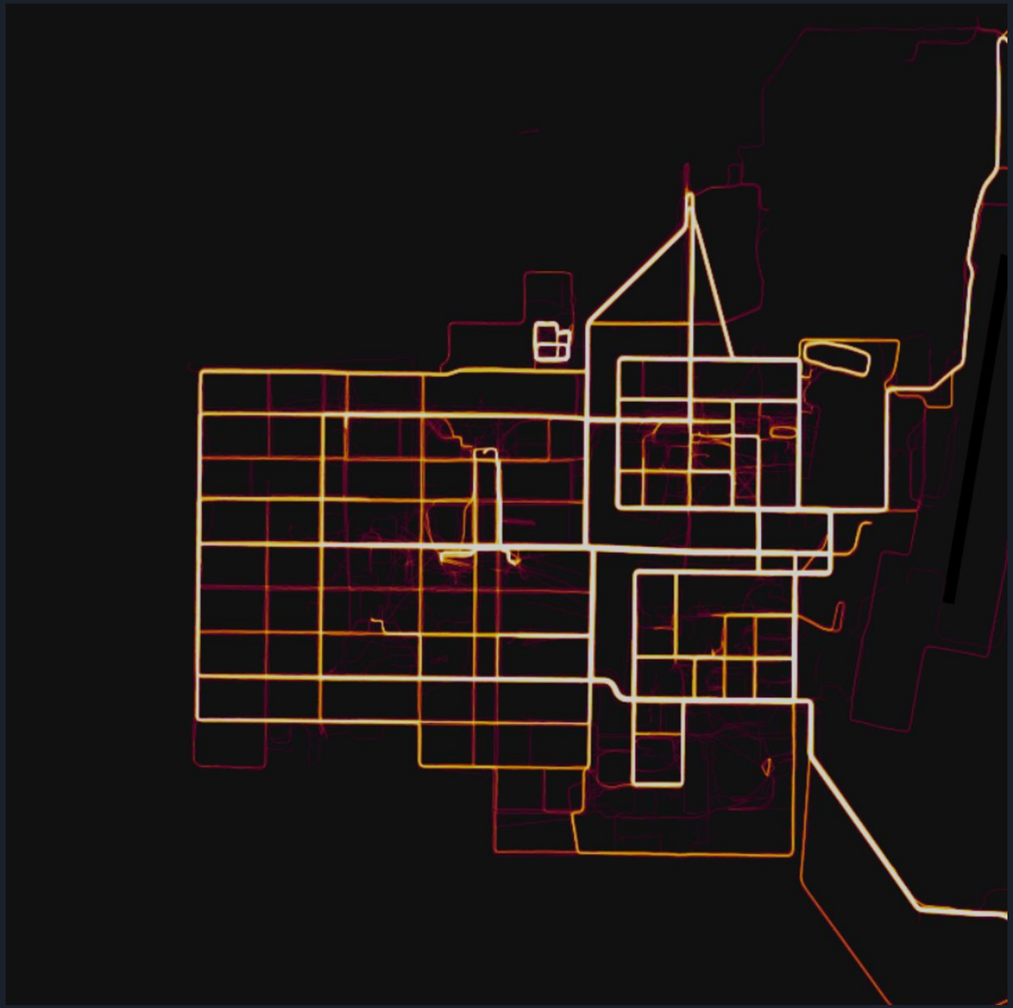
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



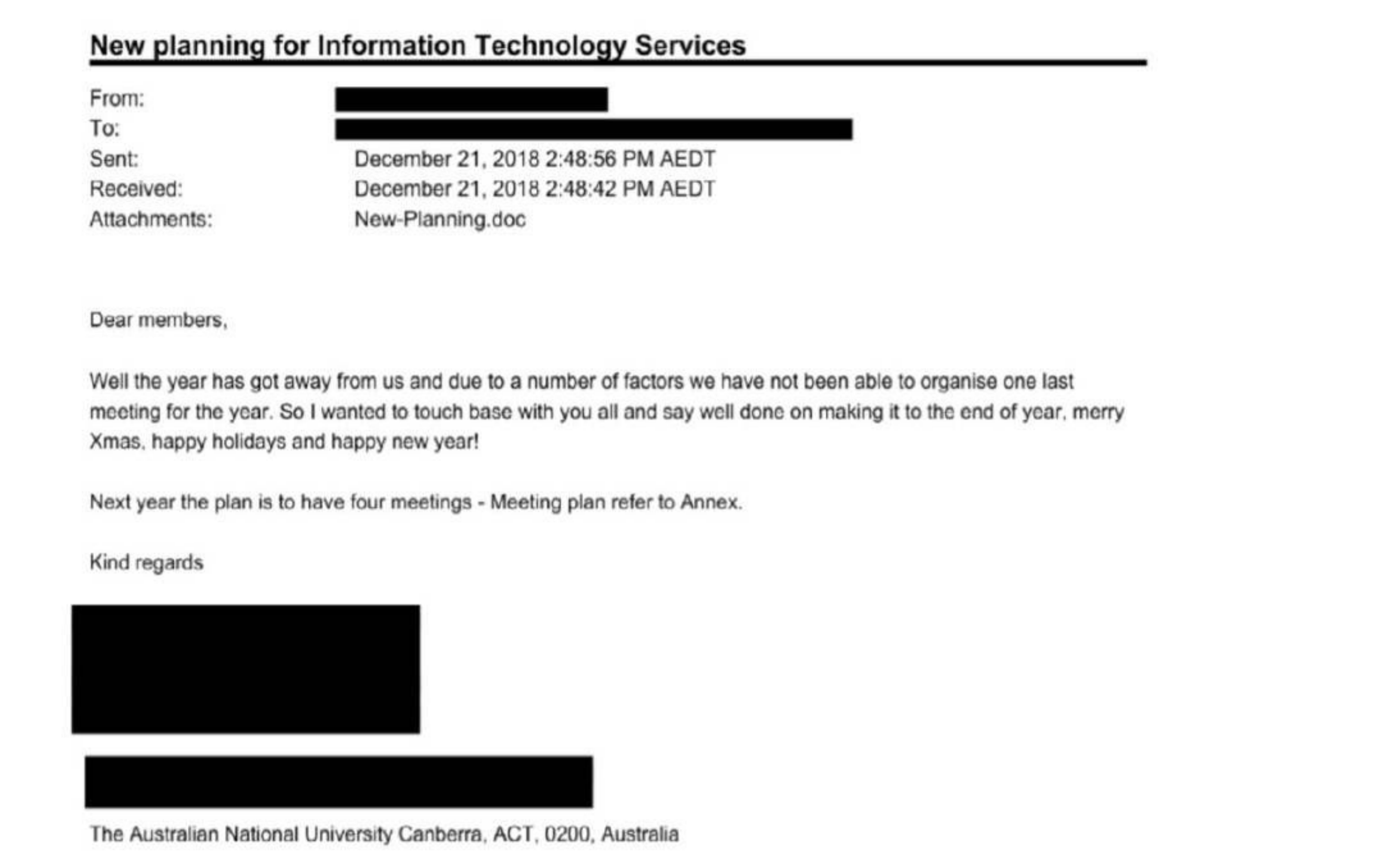


Malware Cyberattacks Targeting Ukraine

2018
Strava



2019
ANU



New planning for Information Technology Services

From: [redacted]
To: [redacted]
Sent: December 21, 2018 2:48:56 PM AEDT
Received: December 21, 2018 2:48:42 PM AEDT
Attachments: New-Planning.doc

Dear members,

Well the year has got away from us and due to a number of factors we have not been able to organise one last meeting for the year. So I wanted to touch base with you all and say well done on making it to the end of year, merry Xmas, happy holidays and happy new year!

Next year the plan is to have four meetings - Meeting plan refer to Annex.

Kind regards

[redacted]

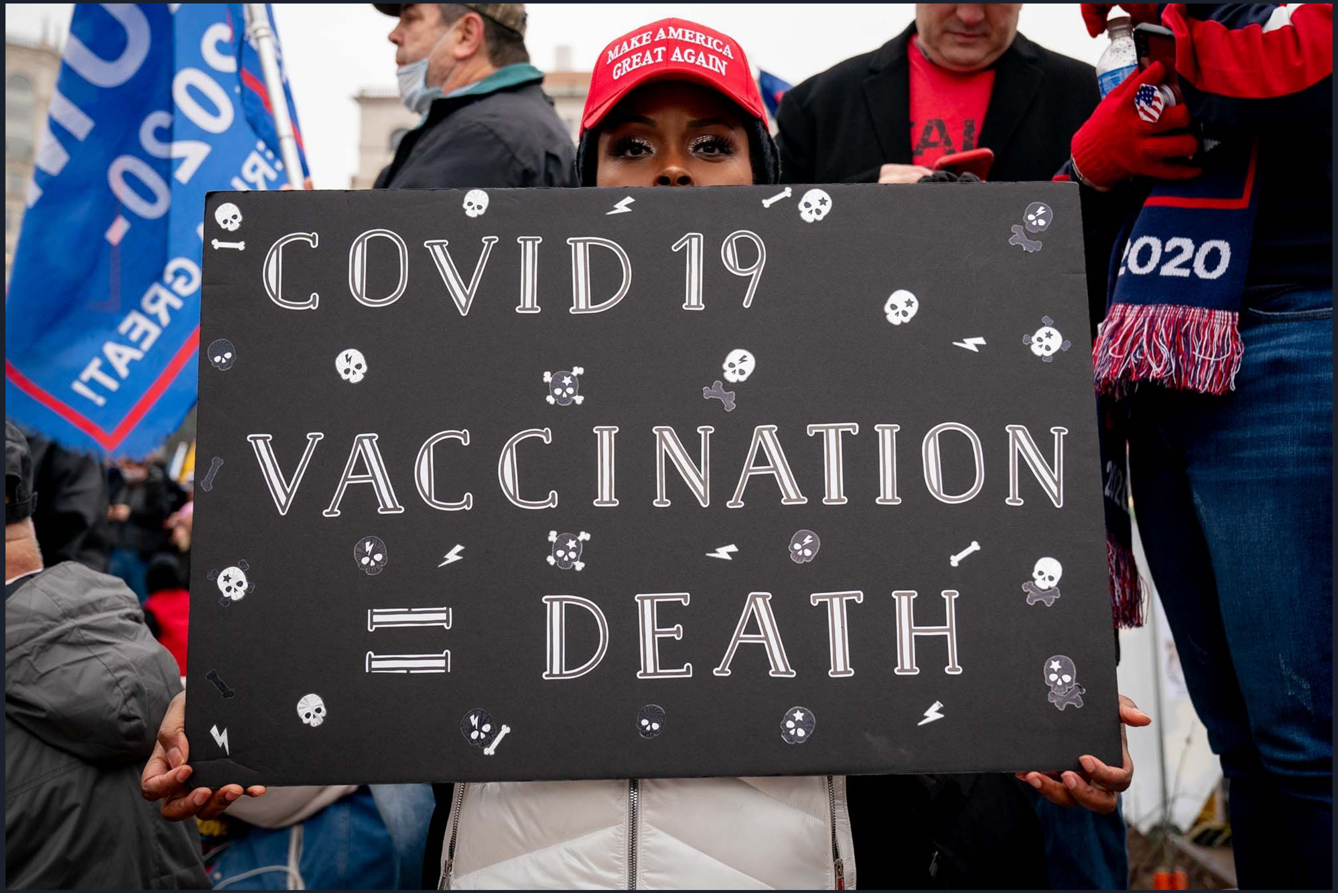
[redacted]

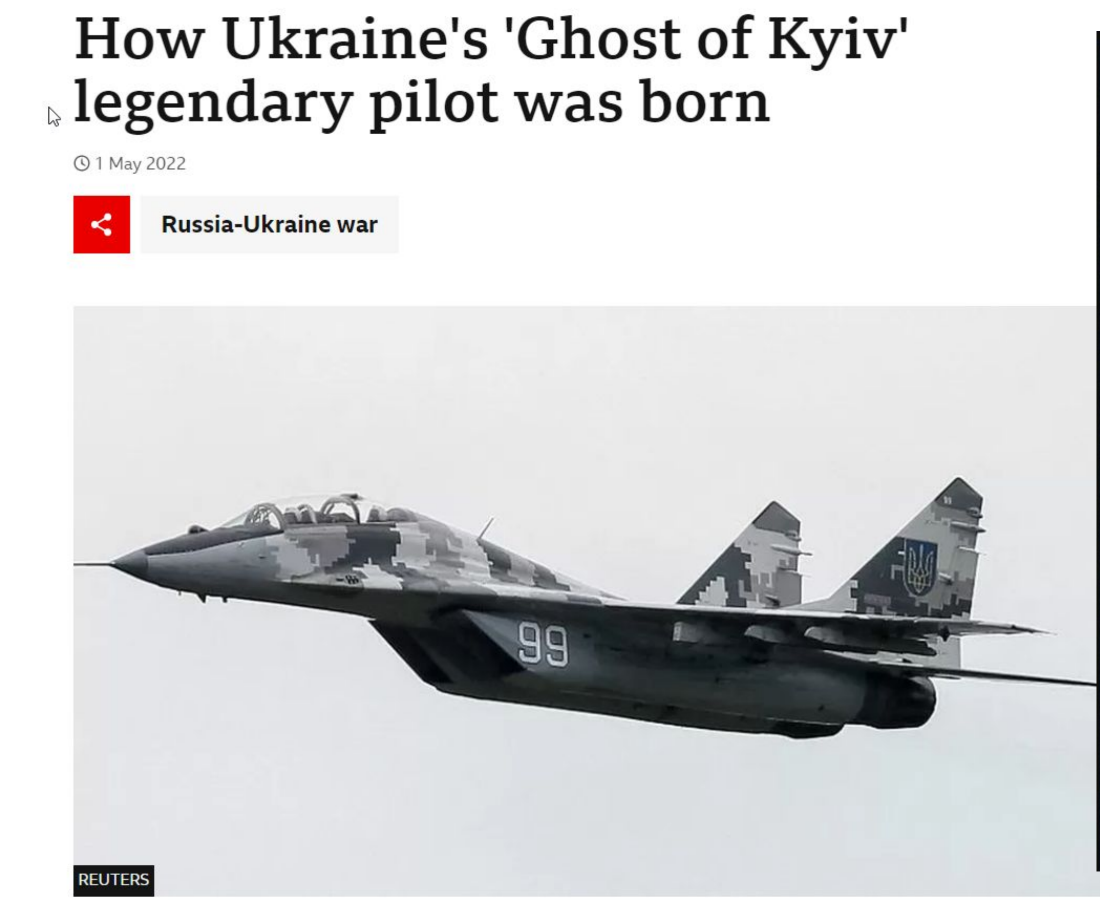
The Australian National University Canberra, ACT, 0200, Australia

“Sophisticated”

“File-less malware”

2020
Misinformation





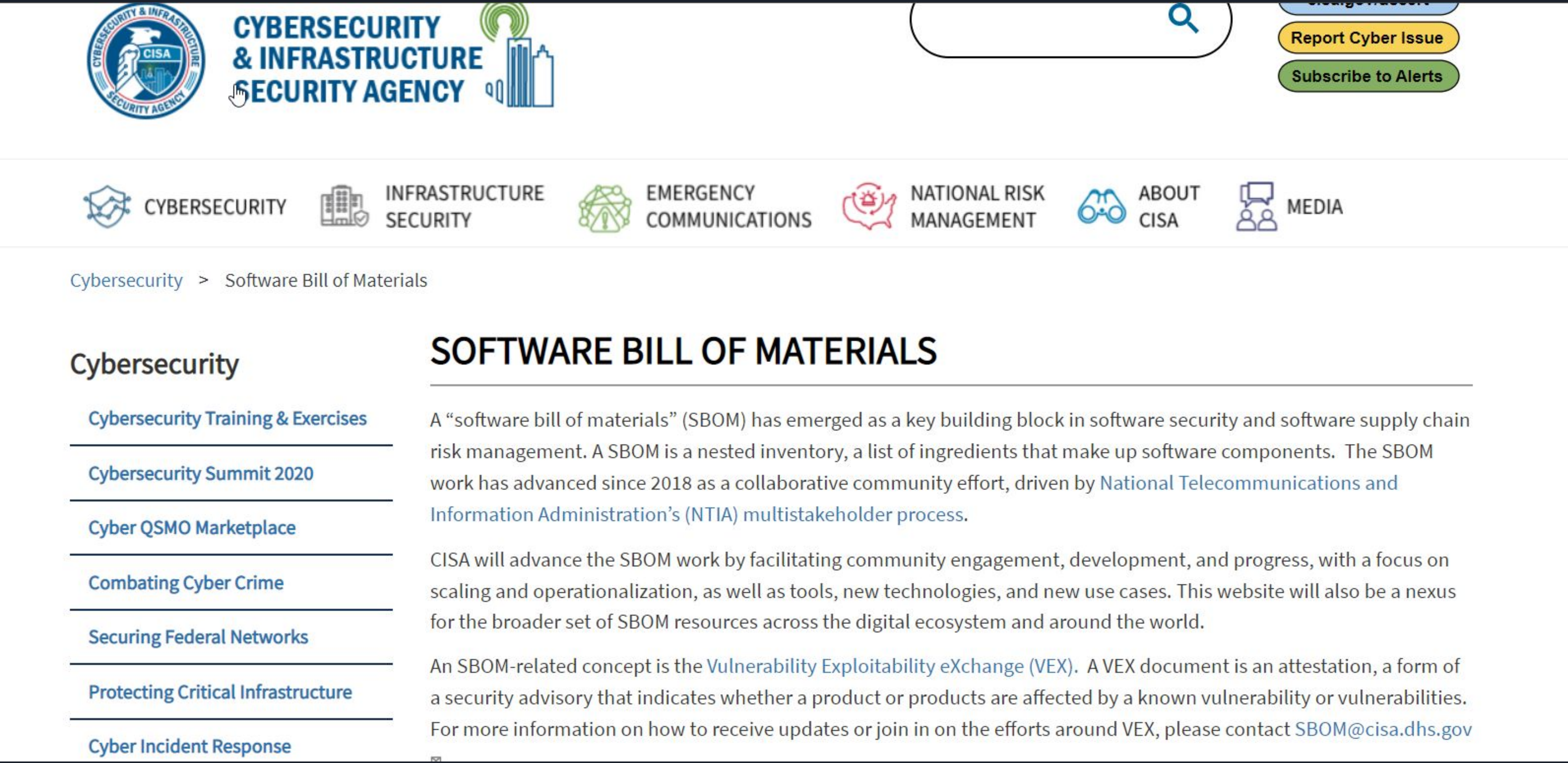
How Ukraine's 'Ghost of Kyiv' legendary pilot was born

1 May 2022

Russia-Ukraine war

REUTERS

2021
Log4J



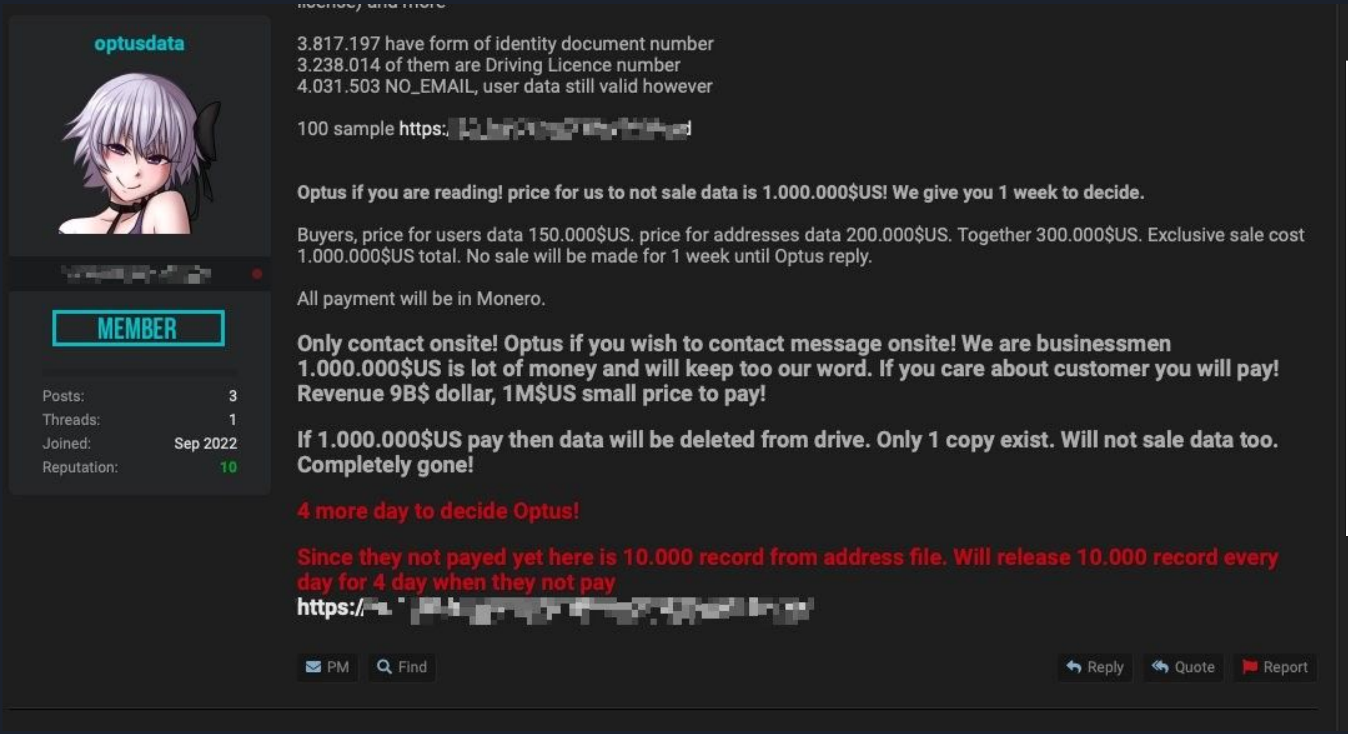
SOFTWARE BILL OF MATERIALS

A "software bill of materials" (SBOM) has emerged as a key building block in software security and software supply chain risk management. A SBOM is a nested inventory, a list of ingredients that make up software components. The SBOM work has advanced since 2018 as a collaborative community effort, driven by National Telecommunications and Information Administration's (NTIA) multistakeholder process.

CISA will advance the SBOM work by facilitating community engagement, development, and progress, with a focus on scaling and operationalization, as well as tools, new technologies, and new use cases. This website will also be a nexus for the broader set of SBOM resources across the digital ecosystem and around the world.

An SBOM-related concept is the Vulnerability Exploitability eXchange (VEX). A VEX document is an attestation, a form of a security advisory that indicates whether a product or products are affected by a known vulnerability or vulnerabilities. For more information on how to receive updates or join in on the efforts around VEX, please contact SBOM@cisa.dhs.gov

2022
Optus vs. Medibank



optusdata

[redacted]

MEMBER

Posts: 3
Threads: 1
Joined: Sep 2022
Reputation: 10

license) and more

3.817.197 have form of identity document number
3.238.014 of them are Driving Licence number
4.031.503 NO_EMAIL, user data still valid however

100 sample https:[redacted]

Optus if you are reading! price for us to not sale data is 1.000.000$US! We give you 1 week to decide.

Buyers, price for users data 150.000$US. price for addresses data 200.000$US. Together 300.000$US. Exclusive sale cost 1.000.000$US total. No sale will be made for 1 week until Optus reply.

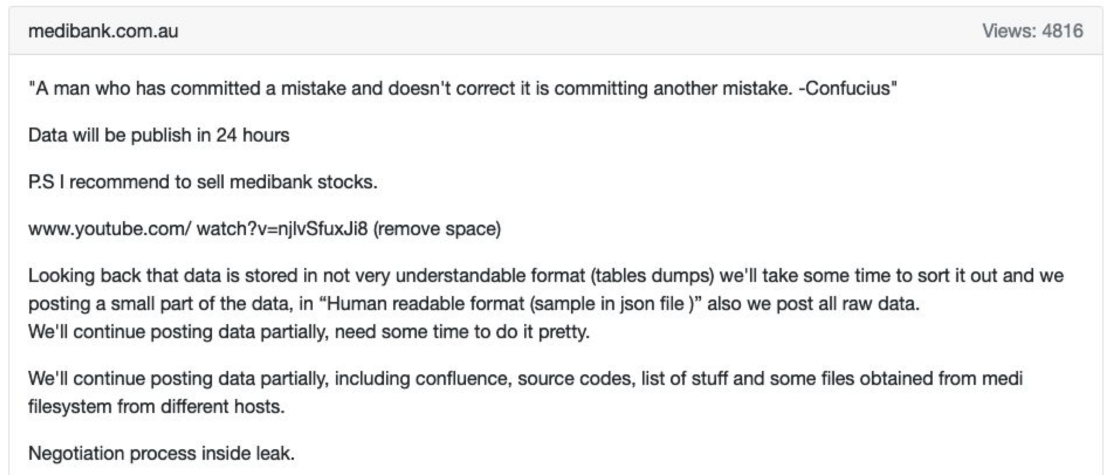
All payment will be in Monero.

Only contact onsite! Optus if you wish to contact message onsite! We are businessmen 1.000.000$US is lot of money and will keep too our word. If you care about customer you will pay! Revenue 9B$ dollar, 1M$US small price to pay!

If 1.000.000$US pay then data will be deleted from drive. Only 1 copy exist. Will not sale data too. Completely gone!

4 more day to decide Optus!

Since they not payed yet here is 10.000 record from address file. Will release 10.000 record every day for 4 day when they not pay
https:/[redacted]



medibank.com.au Views: 4816

"A man who has committed a mistake and doesn't correct it is committing another mistake. -Confucius"

Data will be publish in 24 hours

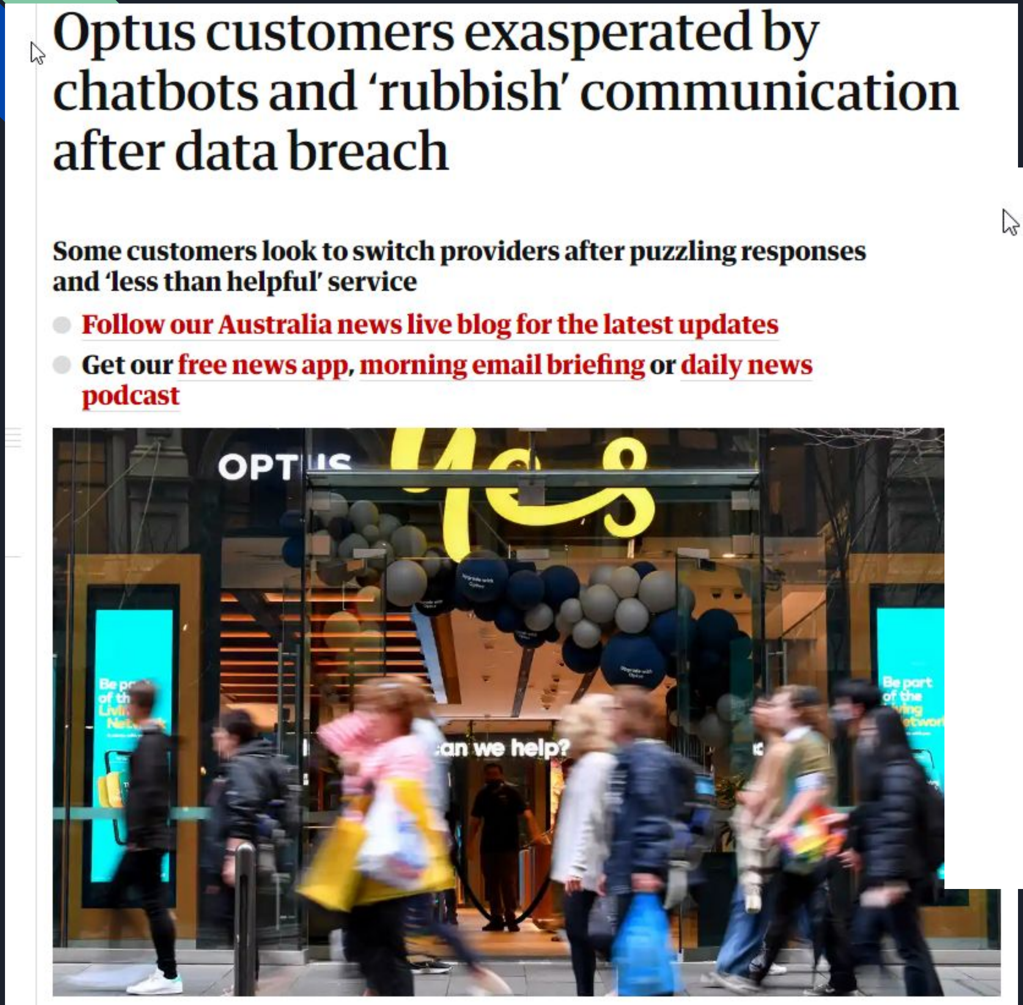
P.S I recommend to sell medibank stocks.

www.youtube.com/ watch?v=njlvSfuxJi8 (remove space)

Looking back that data is stored in not very understandable format (tables dumps) we'll take some time to sort it out and we posting a small part of the data, in "Human readable format (sample in json file)" also we post all raw data.
We'll continue posting data partially, need some time to do it pretty.

We'll continue posting data partially, including confluence, source codes, list of stuff and some files obtained from medi filesystem from different hosts.

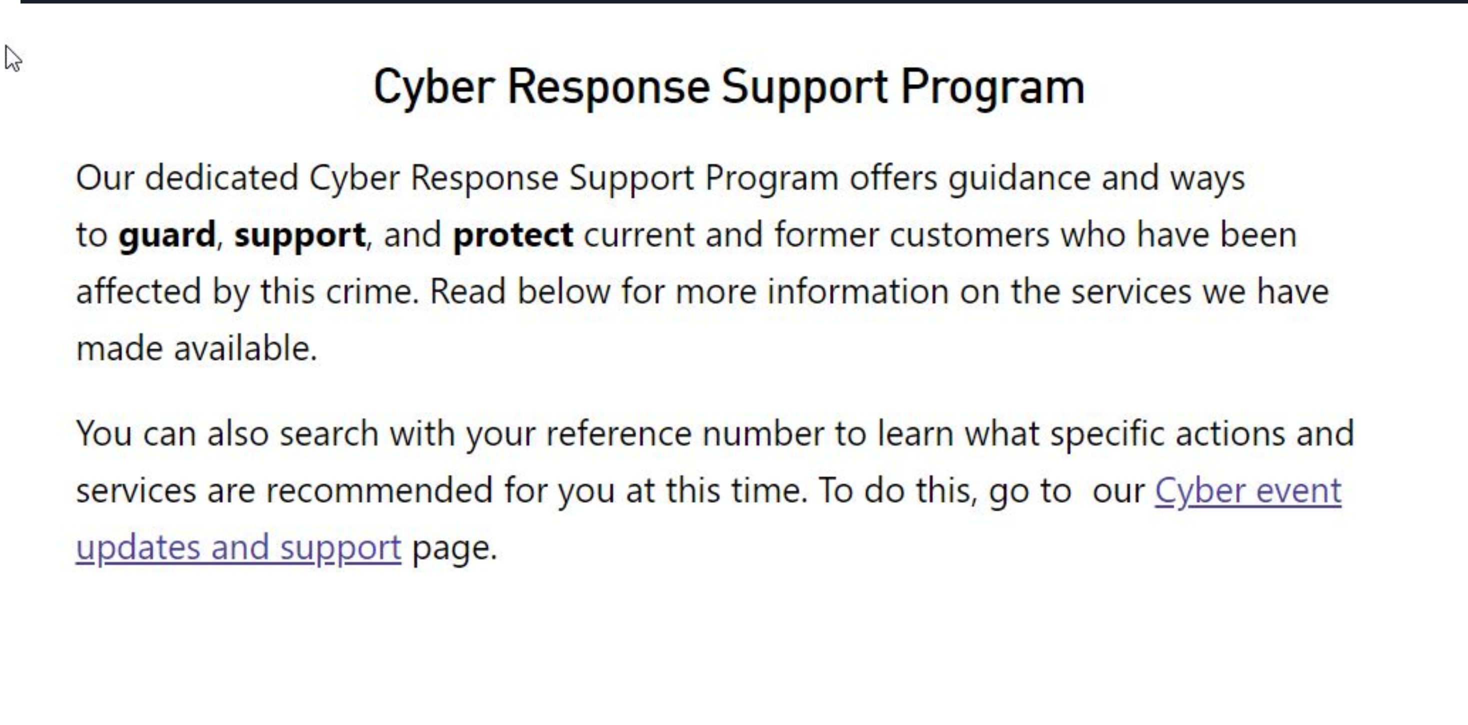
Negotiation process inside leak.



Optus customers exasperated by chatbots and 'rubbish' communication after data breach

Some customers look to switch providers after puzzling responses and 'less than helpful' service

- **Follow our Australia news live blog for the latest updates**
- **Get our free news app, morning email briefing or daily news podcast**



Cyber Response Support Program

Our dedicated Cyber Response Support Program offers guidance and ways to **guard**, **support**, and **protect** current and former customers who have been affected by this crime. Read below for more information on the services we have made available.

You can also search with your reference number to learn what specific actions and services are recommended for you at this time. To do this, go to our Cyber event updates and support page.

Summary

I LEARN FROM MY MISTAKES

I LEARN FROM OTHER PEOPLE'S MISTAKE

I LEARN FROM EVERYONE'S MISTAKE INCLUDING MY OWN

[redacted]

i learn from the mistakes of people who took my advice

Thanks!

icd@wan0.net
@wan0net