Ransomware Awareness

for Hampshire Secondary Schools

Hampshire County Council and Project Knapweed

1 December 2023

Today's Presenters

Bruce Thomson

Bruce's background is in cyber security and digital forensics, he has worked in local government, and has coded a number of Open Source cyber security tools. Since 2020, he has focused on ransomware attacks and their impact on the UK public sector, and is the founder of Project Knapweed, a small team of pro-bono specialists that seek to help UK public sector organisations that have been impacted by ransomware attacks.

David Wigley

David is an Enterprise Architect at Hampshire County Council, where he has worked for nearly 30 years. In that time he's designed all the networks and most of the security systems used by the Council including HPSN which was used by most Hampshire schools. David has over a decade of experience in cyber security, security architecture and compliance.

Rob Tillman

Rob is a Senior Security Specialist within Hampshire County Council, his day-to-day duties tend to be on the operational front and include management of the Security Information and Event Management platform, dealing with vulnerability and threat intelligence and ensuring new solutions are secure before go live.   Rob has worked within IT at the Council for almost 25 years, in varying different technical roles.

Agenda

1. Introduction to Ransomware	2. Ransomware in the Wild	3. Prepare for Ransomware
The evolution of ransomware	Real world experience	Proactive Steps
Why it is important to know	Project Knapweed	Technical Controls
Attack on a Hampshire School	Impact to People	What to do in worst case scenario
Short break	*Break & Dark web demo*	*Summary & Questions*

Seminar format and approach

1) This is friendly advice, not a sales pitch.

2) We’ll try to avoid scare tactics, but ransomware is scary.

3) Our aim is to raise awareness of the threat from ransomware.

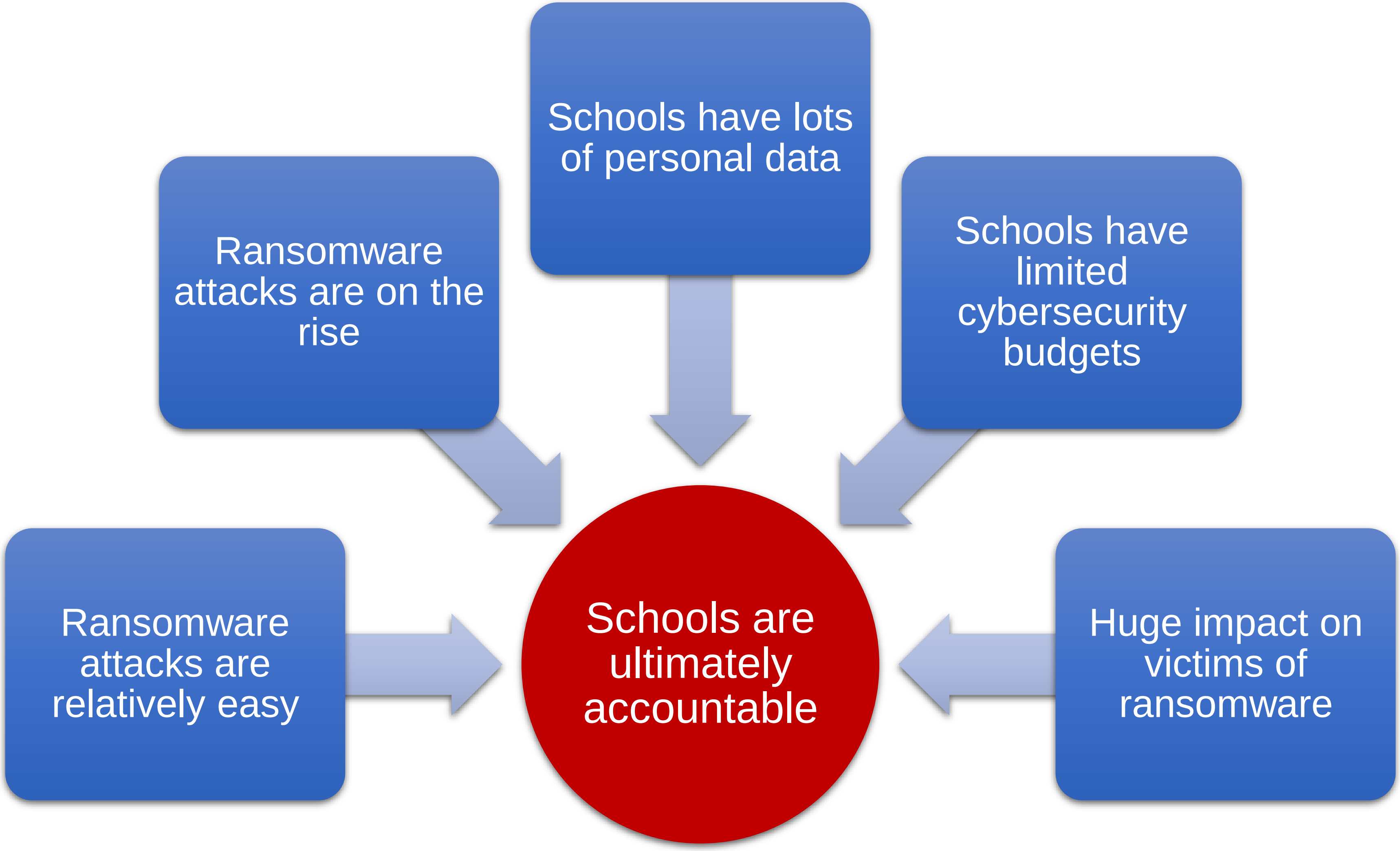
4) We’ll also share practical steps to reduce your risk.

5) We have a lot of content, so we’ll take regular breaks.

6) Questions are welcome throughout.

7) You’ll also have the chance to delve into the Dark web with Bruce during the break.

Why it’s important to know about Ransomware



Schools have lots of personal data

Ransomware attacks are on the rise

Schools have limited cybersecurity budgets

Ransomware attacks are relatively easy

Schools are ultimately accountable

Huge impact on victims of ransomware

Part 1

Introduction to Ransomware

David Wigley

Hampshire County Council

What is Ransomware

Definition

Ransomware is a distinct type of malware (malicious software) that aims to prevent you from accessing your device and the data stored upon it, by encrypting your files.

The device itself may become locked, or the data on it might be encrypted, stolen or deleted.

The attacker will then demand a ransom in exchange for the decryption of data. They may also threaten to leak the data they steal.

Ransomware

=

Blackmail

Evolution of Ransomware

1989

First recorded ransomware, created by Dr. Joseph Popp and distributed to 20,000 attendees at the World Health Organization AIDS conference (on floppy disks).

2013

CryptoLocker was the first ransomware to demand payment in bitcoin.

2016

Locky was the first widespread ransomware. Up to 500,000 phishing emails sent out per day.

2017

WannaCry and NotPetya infect c200,000 computers across 15 countries (North Korea blamed).

NotPetya mainly targeted Ukraine (US officials estimate more than $10B damages).

WannaCry significantly impacted the UK NHS.

2020

In response to improved backups by ransomware targets, attackers start to steal data and threaten to leak or sell it on the Dark web.

2021

DarkSide attack shuts down Colonial oil pipeline for 6 days. $4.4M bitcoin ransom paid.

2022 to 2023

Successful ransomware attack on at least two Hampshire Secondary Schools.

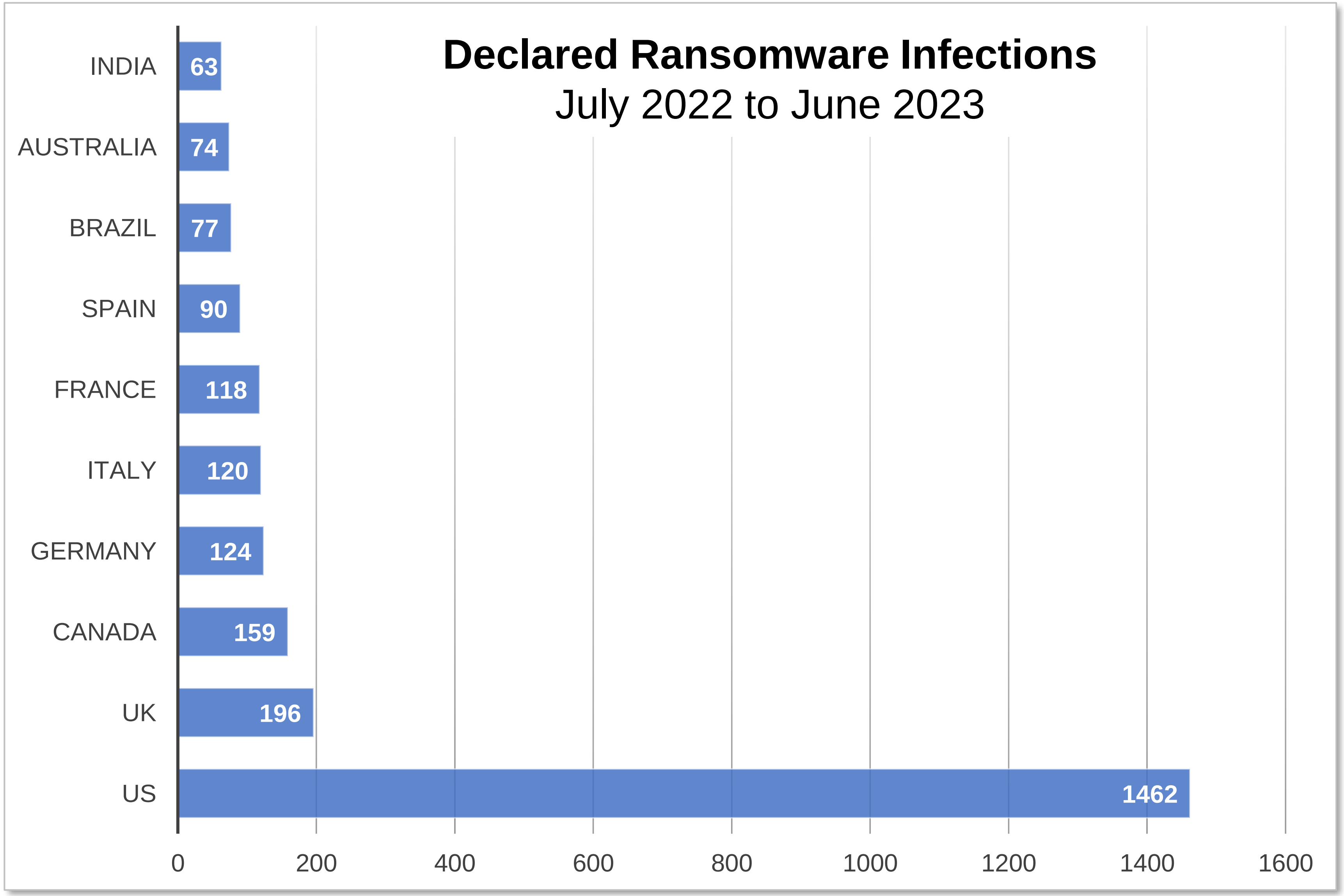
Sources: ransomware.org, NCSC and Project Knapweed

Who’s being attacked?

Over the last 12 months, the UK is the second most targeted country for Ransomware attack.

The number of UK declared infections is disproportionately high, compared with our size.

Note: Number of actual infections is likely to be higher than the number declared.



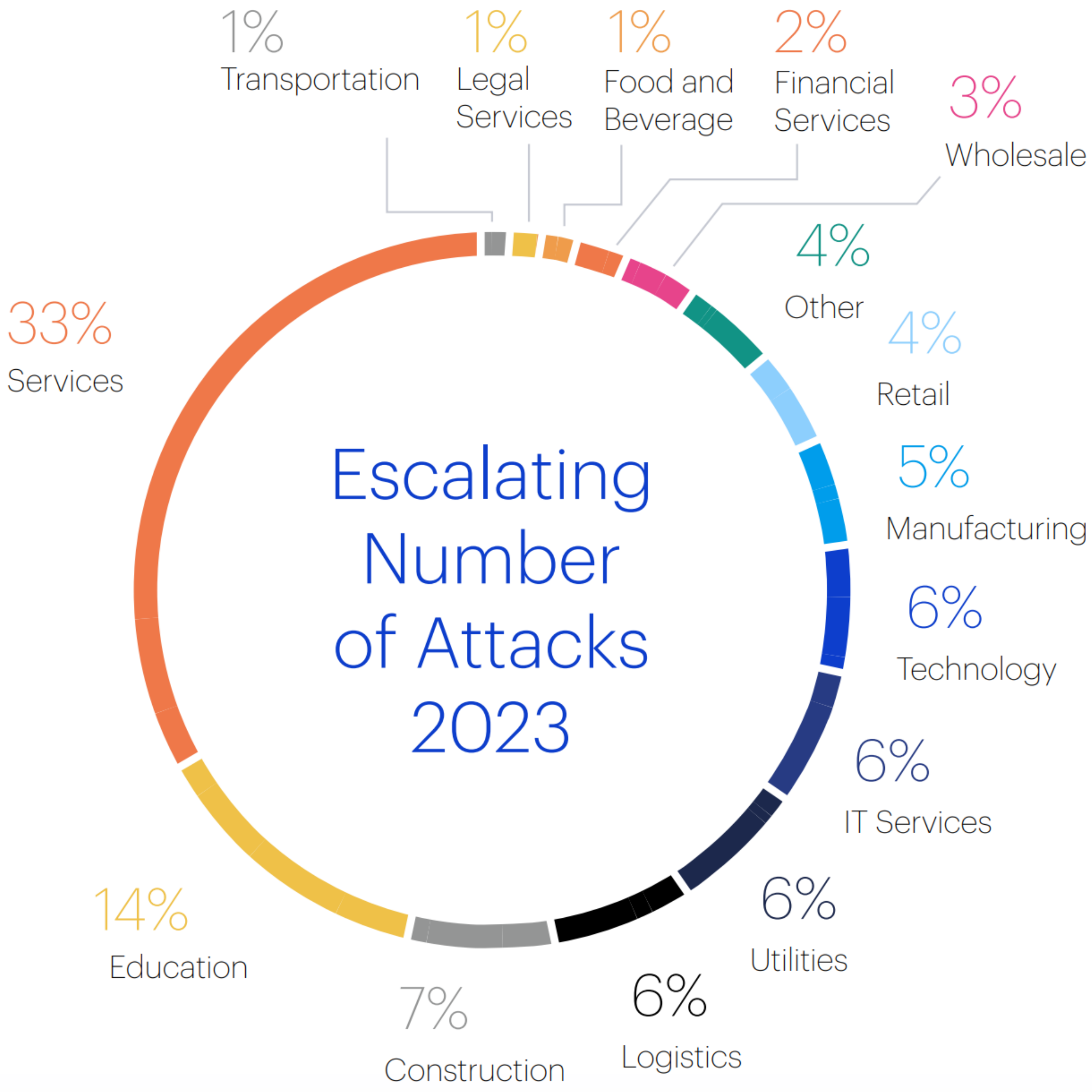
Source: Malwarebytes Ransomware Report for UK 2023.

Who's being attacked in the UK?

Over the last 12 months, education was the second most attacked sector in the UK, a far higher proportion than in other countries, including the US.

Education has lots of personal data, but limited cybersecurity funding.

Ability to target the data of younger people (more on that in **Part 2**).



Source: Malwarebytes Ransomware Report for UK 2023.

Ransomware in the Wild

Project Knapweed constantly monitors the Dark web, looking for posts from 163 ransomware groups about who they've compromised.

10
in 24 hours

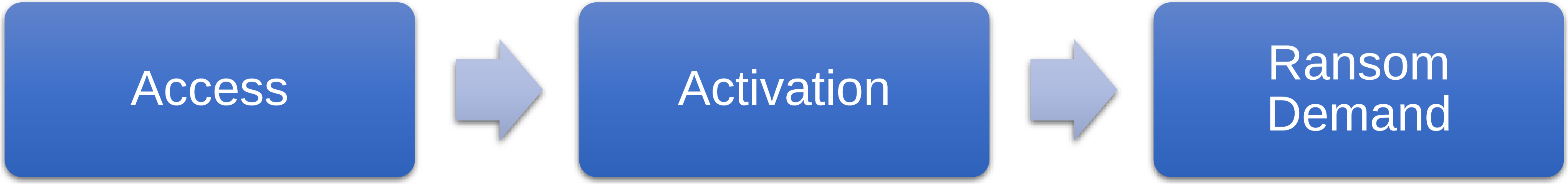
349
in November

1371
in 3 months

4271
in 2023

Source: Project Knapweed

How does it work?



Access

Activation

Ransom Demand

Attackers gain access to your network (usually through email phishing or insecure remote access).

They then plant malicious encryption software (ransomware).

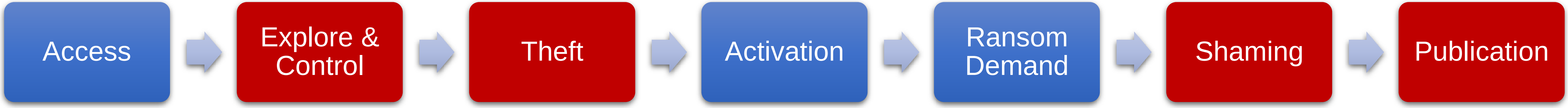
The malware is activated, locking devices and causing the data across the network to be encrypted, so you can no longer access it.

This can spread across a network of connected computers in minutes.

Usually you receive an on-screen notification, explaining the ransom and how to make the payment to unlock your computer or regain access to your data.

Payment is usually via an anonymous web page in Bitcoin cryptocurrency.

How does it work now?



Access

Attackers gain access to your network.

They establish control and plant malicious encryption software.

Explore & Control

Attackers move silently across the network, looking for high value data.

They also try to find your backup service and disable it, so you can’t restore.

Also target Office 365 SharePoint file versions so you can’t restore.

Theft

Attackers silently steal your data and copy it to places they control on the Dark web.

Activation

The malware is activated, locking devices and causing the data across the network to be encrypted, so you can no longer access it.

This can spread across a network of connected computers in minutes.

Ransom Demand

You receive an on-screen notification, explaining the ransom and how to make the payment to unlock your computers and data.

They will also threaten to leak your data on the Dark web if you don’t pay.

Shaming

Attackers will often publish the name of your organisation on Dark web forums, telling other cyber criminals that they have your data.

Government agencies, security companies and security researchers monitor these forums.

Publication

If you don’t pay the ransom, the attackers might release your data on the Dark web.

If this is personal data, it is a major data protection breach.

What is the Dark Web?

Surface web is the web that we use all the time. It holds the websites most of us use and is indexed, so you can search it using Google, Bing etc.

Deep web is part of the web that isn’t indexed, so can’t be searched. It holds a lot of legitimate content including web mail, online banking, medical data, video streaming, services behind paywalls etc.

Dark web is used for illegal purposes. You need special software to access it. This is typically where ransomware gangs will advertise, store, sell and leak stolen data.

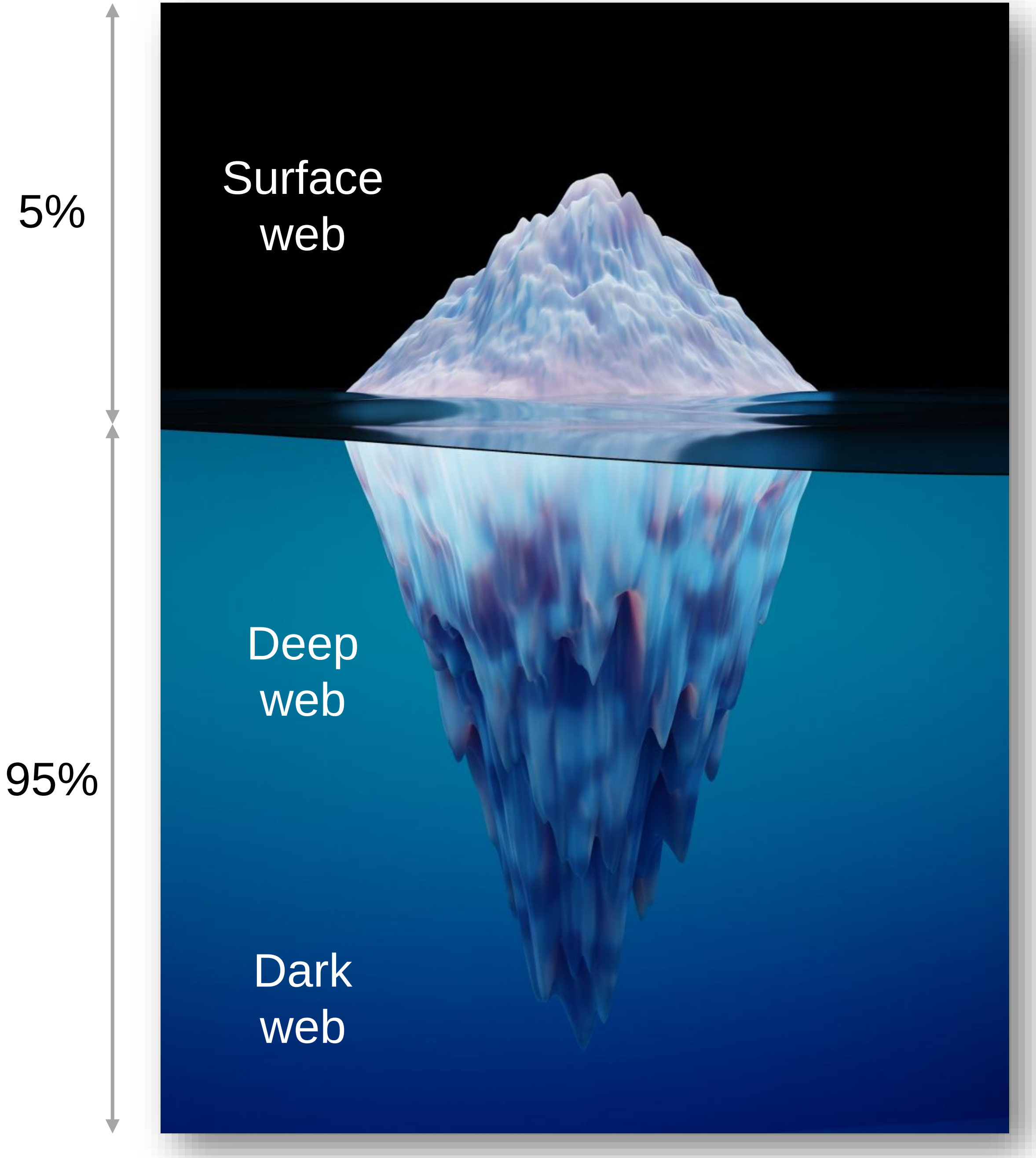


Photo by SIMON LEE on Unsplash

Ransomware Myths

If you pay the ransom, you'll get the data back and it won't be leaked.

It's the attacker's fault, we're just victims.

They won't target schools.

We're safe with Office 365 or G-Suite.

Our suppliers will look after our data.

In reality

Ransomware is a growing threat.

Attacks are up year by year.

The UK is the second biggest target after the US.

Education is the second most targeted sector in the UK.

The impact of a successful attack is **significant**.

Real World Story

The following has been provided by a Hampshire School that was hit by ransomware

At their request, we’re not disclosing their name

Real World Story

Day 1 after Easter holidays – everything was down.

- Ensure IT team are extra vigilant towards end of holidays as it seems a common tactic to hit schools at this time.
- Have a back-up plan. We had used “old-fashioned” SIMS which we could not access. Have set of paper registers ready at all times; we have since moved to online MIS systems, which would have made life easier.
- Having said that, it took a while to get the internet back running, so be prepared to be reduced to nothing!

Real World Story

We were relieved that:

- They were not able to access SIMS
- They were not able to access CPOMS online safeguarding tool
- A great deal of the information was largely useless
- We had a back-up server off site which allowed us to retrieve everything

Real World Story

Tips:

- Be open and honest with staff and families of students.
- Ensure all communication focuses on the actions of criminals and that we are all victims. Anyone is susceptible to these things.
- Reassure parents of information which has definitely NOT been accessed. Many understandably concerned about child protection files etc.
- Ensure you are always “weeding” your files. Out of date files should be deleted in a timely manner.
- Move as much as possible to the cloud.

Real World Story

If it happens to you (I hope it doesn’t):

- Phone ICO helpdesk (they advised to report through “Action Fraud”)
- Report to National Cyber Security Centre
- Inform police (very little resource to support)
- Inform Local Authority
- Take advice on preparing a press statement – I managed to see off some Sun journalists by reassuring them there was not story.
- Bruce and the Knapweed team were an absolute godsend! Listen to their calm reassurances and follow their wise advice.

Part 2

Ransomware in the Wild

Bruce Thomson

Project Knapweed

dark web/ransomware beyond that initial cyber attack

the evolution of the Knapweed fusion cell

Contents TLP:Amber

Original work by @cryptomoose
Jan – December: 2023

The back story

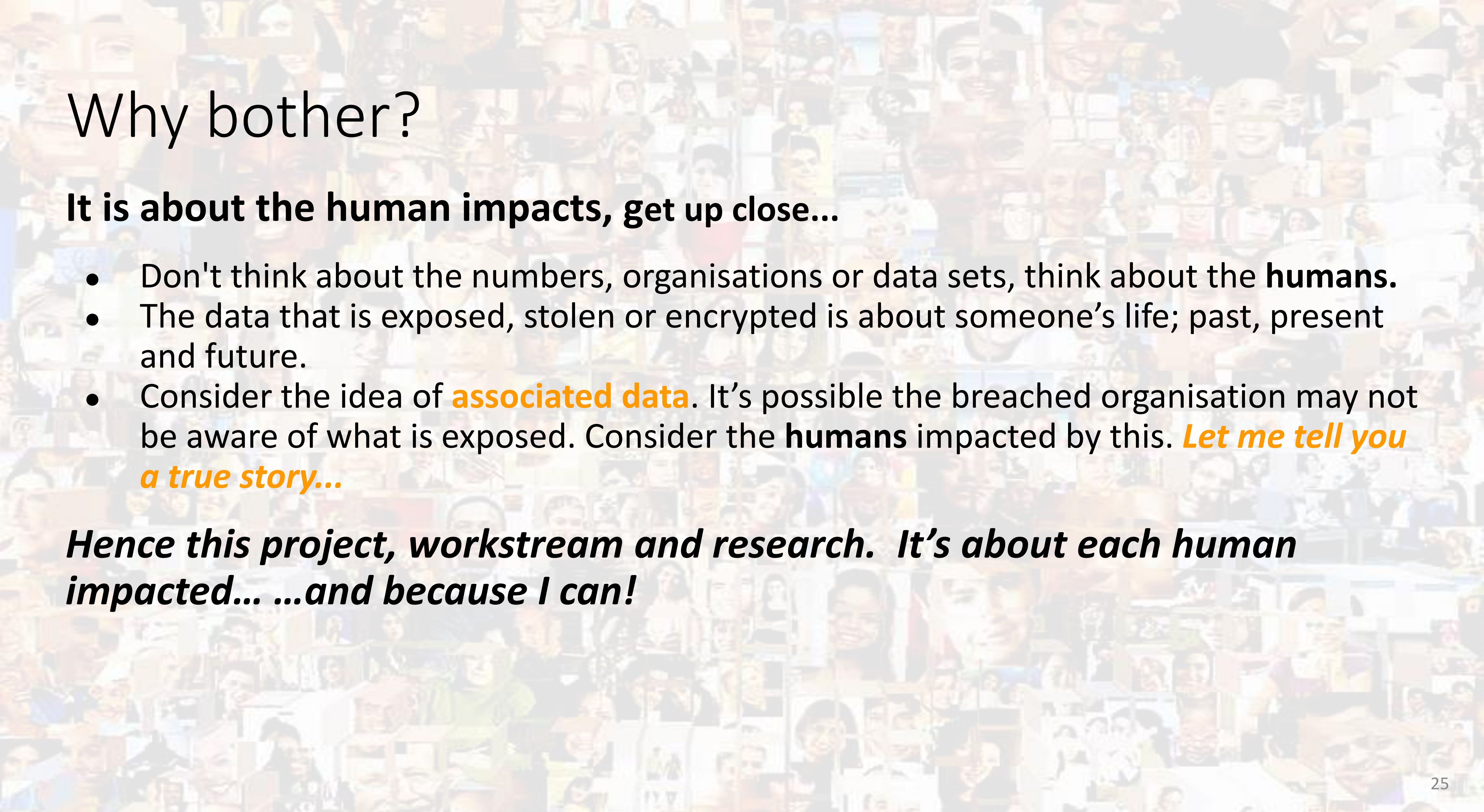
1. Autumn of 2019 I was researching the dark web. Early in 2020 I was presenting on “standard crime”, all the usual stuff, weapons, drugs, and pornography to a number of public sector cyber security forums around the UK, and preparing to revisit in the summer/autumn 2020

2. Poor quality dark web/ransomware data:
   - Opens the door to snake-oil sales, “we have seen your email on the dark web, buy our service”! These are often poor, with no context, no password, no dates, no sites, no history of very much.
   - SIEMs and SOC integrations and thread feeds are often very poor, impacting Sentinel, AV USM, Splunk and others.

These two strands led me to what has now become ***Project Knapweed****.* *(est Feb 2023)*

Project Knapweed: why bother?

- **The UK Public Sector is often told *we* have people who do this. If so, they do not seem to share things very well!**
  - *Therefore, it would be good to see what may be discoverable and recoverable from the dark web ransomware groups and share this with the broader UK Public Sector who suffer from these attacks - and their data being on these sites.*
  - *This can be done via the CyberSec forums/WARPs and other Public Sector groups and organisations.*
- **To better understand the concept and risk of "associated data".**
  - *The personal and organisational impacts from somebody else's breach.*
  - *Consider your data exfiltrated and exposed to the dark web. The victims of the ransomware incident are not aware of what was exfiltrated so they can't tell you or the ICO.*
- **To understand what open source tools are available, the time needed to support this work and the subsequent support to those impacted:**
  - *The cost of running them (TCO, capital and revenue expenditure).*
  - *The cost, time and rigour of reporting.*
  - *The moral, ethical and legal positions.*



Why bother?

It is about the human impacts, get up close…

- Don't think about the numbers, organisations or data sets, think about the **humans.**
- The data that is exposed, stolen or encrypted is about someone’s life; past, present and future.
- Consider the idea of **associated data**. It’s possible the breached organisation may not be aware of what is exposed. Consider the **humans** impacted by this. ***Let me tell you a true story…***

Hence this project, workstream and research. It’s about each human impacted… …and because I can!

Why bother?

Ransomware attacks on schools are increasingly preceded by the exfiltration of personal information to feed the big data files used to inform

Ransomware and AI driven crime:

By the time pupils are old enough to apply for a bank account/credit card/student loan that may already been organised by someone else with their data leaving them on a digital bad-credit-risk list (the e-death penalty), probably after a breach which may not have been known or reported.

Why bother?

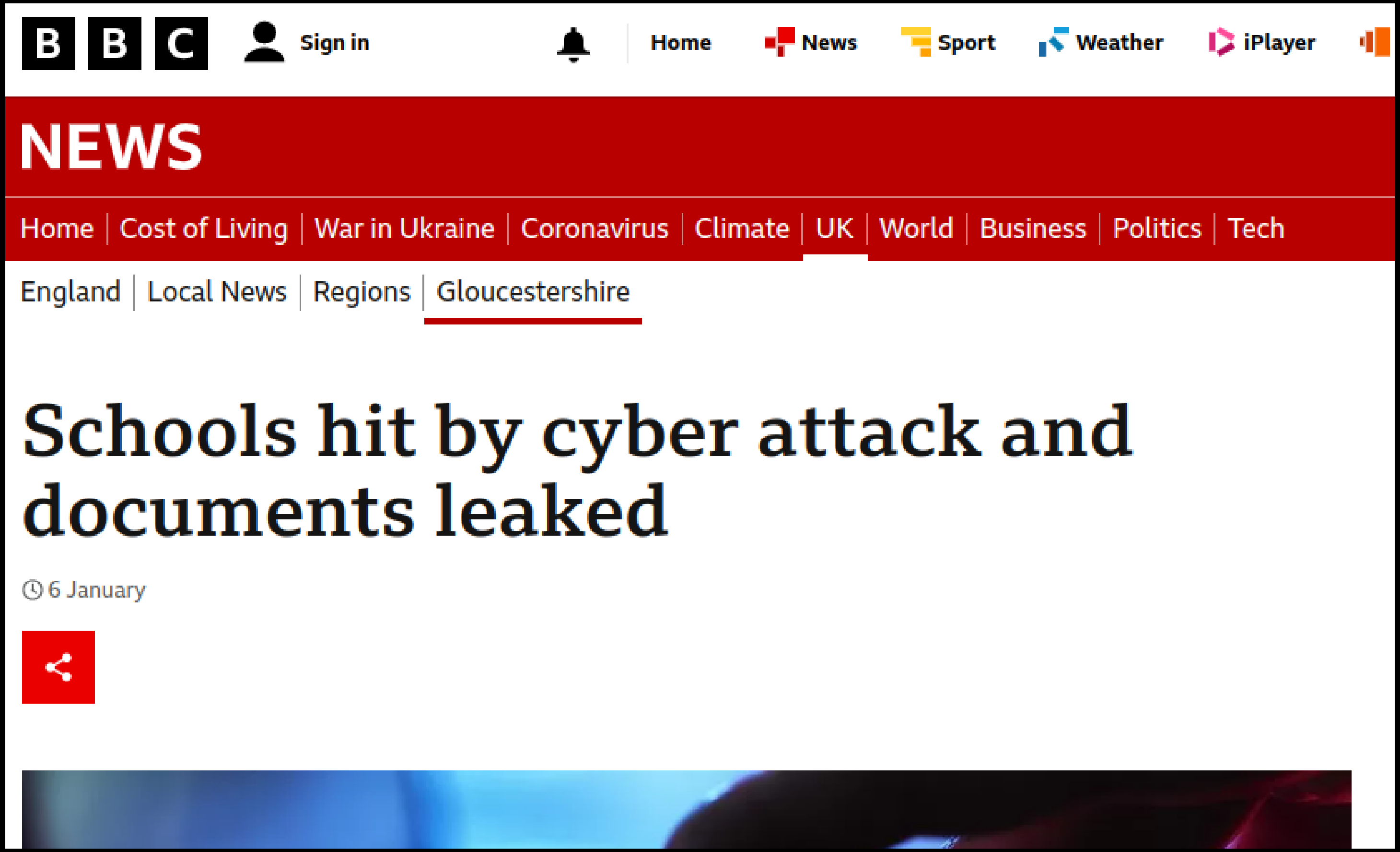
Administrator FRP Advisory Trading Limited said about **730 employees would be made redundant**. They said June's cyber attack had damaged KNP Logistic Group's financial position and its ability to secure additional investment and funding.

KNP Logistics Group was formed in 2016 when Knights of Old merged with Derby-based Nelson Distribution Limited, Knights of Old started out as a single horse and cart in 1865 and is one of the UK's largest privately owned logistics companies.

https://www.bbc.co.uk/news/uk-england-northamptonshire-66927965

So who is attacking schools? – 6th Jan BBC

- Carmel College, St Helens
- Durham Johnston Comprehensive School
- Frances King School of English, London/Dublin
- Gateway College, Hamilton, Leicester
- Holy Family RC + CE College, Heywood
- Lampton School, Hounslow, London
- Mossbourne Federation, London
- Pilton Community College, Barnstaple
- Samuel Ryder Academy, St Albans
- School of Oriental and African Studies, London
- St Paul's Catholic College, Sunbury-on-Thames
- Test Valley School, Stockbridge
- The De Montfort School, Evesham

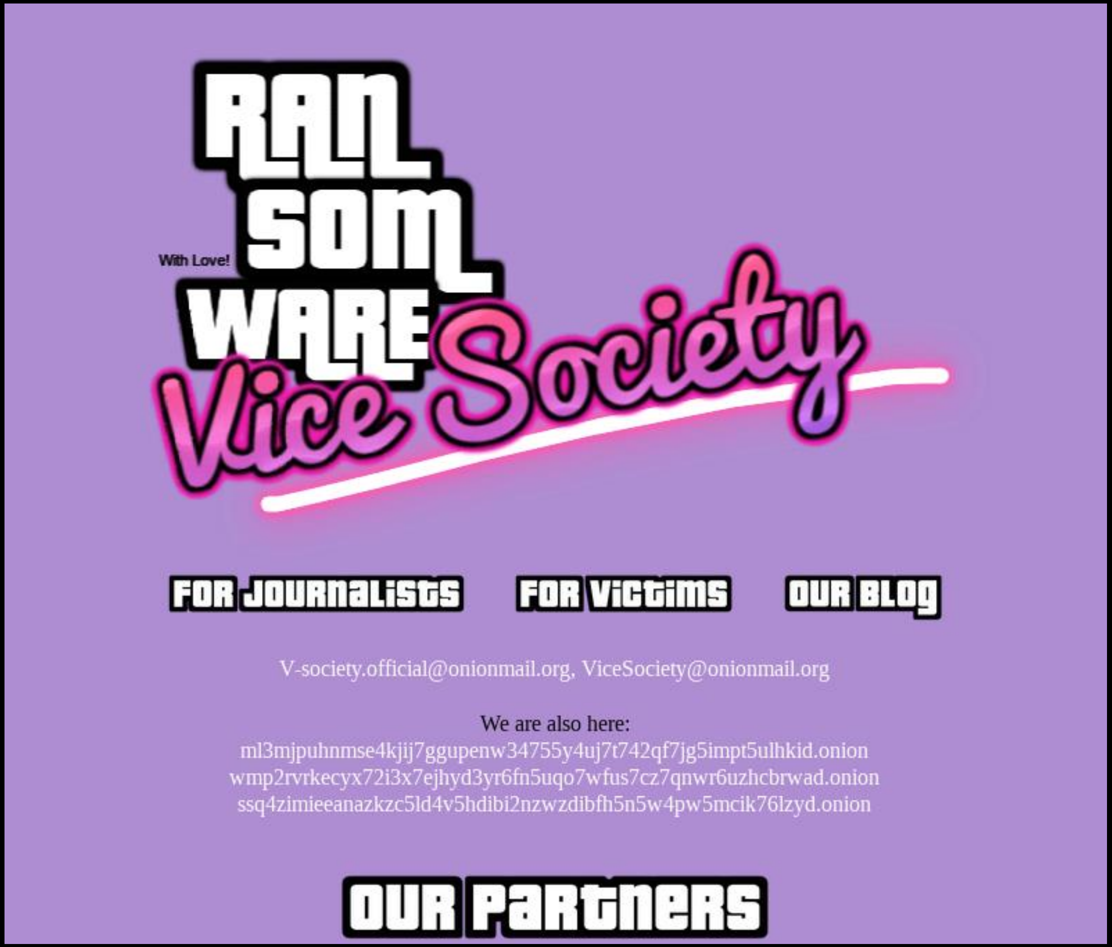

BBC
Sign in
Home
News
Sport
Weather
iPlayer
NEWS
Home | Cost of Living | War in Ukraine | Coronavirus | Climate | UK | World | Business | Politics | Tech
England | Local News | Regions | Gloucestershire

Schools hit by cyber attack and documents leaked

6 January

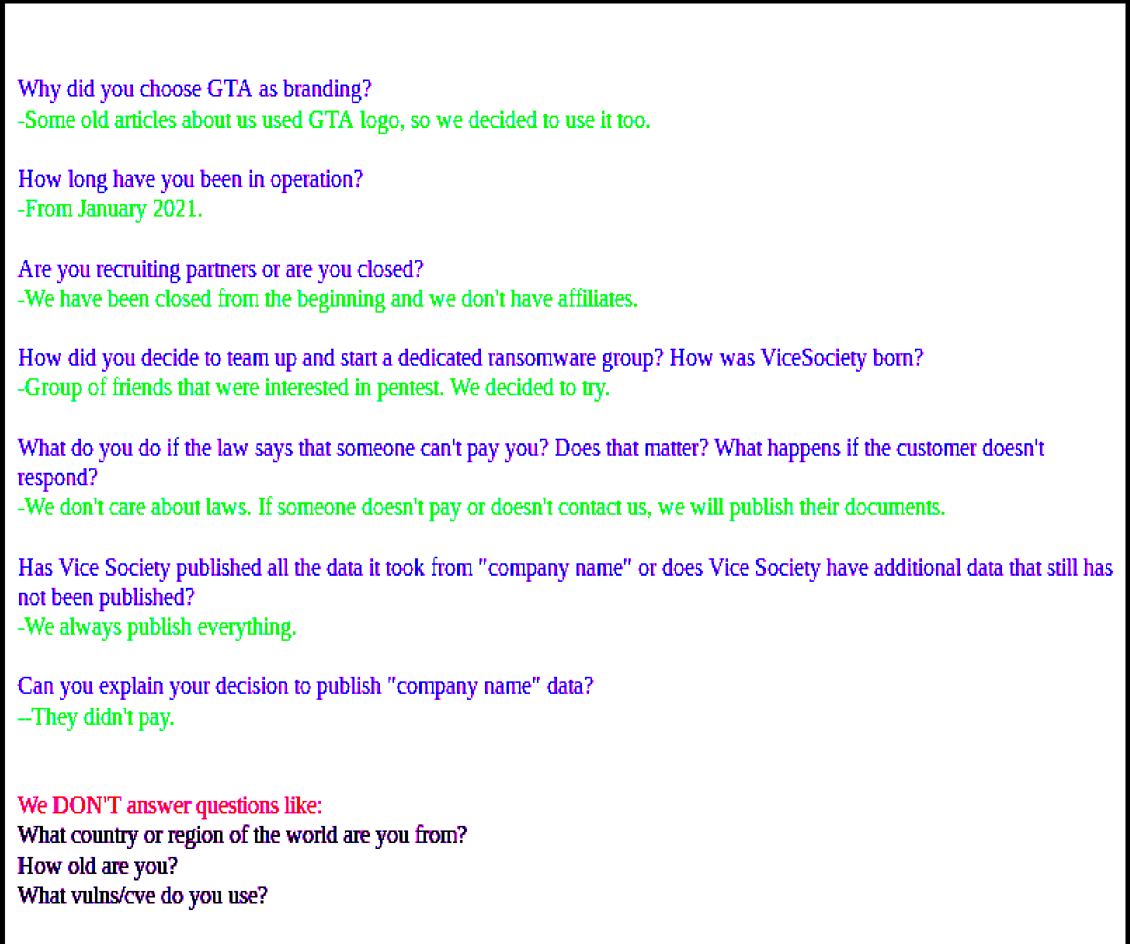
https://www.bbc.co.uk/news/uk-england-gloucestershire-63637883

Meet Vice Society – *there are others:*



V-society.official@onionmail.org, ViceSociety@onionmail.org

We are also here:
ml3mjpuhnmse4kjij7ggupenw34755y4uj7t742qf7jg5impt5ulhkid.onion
wmp2rvrkecyx72i3x7ejhyd3yr6fn5uqo7wfus7cz7qnwr6uzhcbrwad.onion
ssq4zimieeanazkzc5ld4v5hdibi2nzwzdibfh5n5w4pw5mcik76lzyd.onion



Why did you choose GTA as branding?
-Some old articles about us used GTA logo, so we decided to use it too.

How long have you been in operation?
-From January 2021.

Are you recruiting partners or are you closed?
-We have been closed from the beginning and we don't have affiliates.

How did you decide to team up and start a dedicated ransomware group? How was ViceSociety born?
-Group of friends that were interested in pentest. We decided to try.

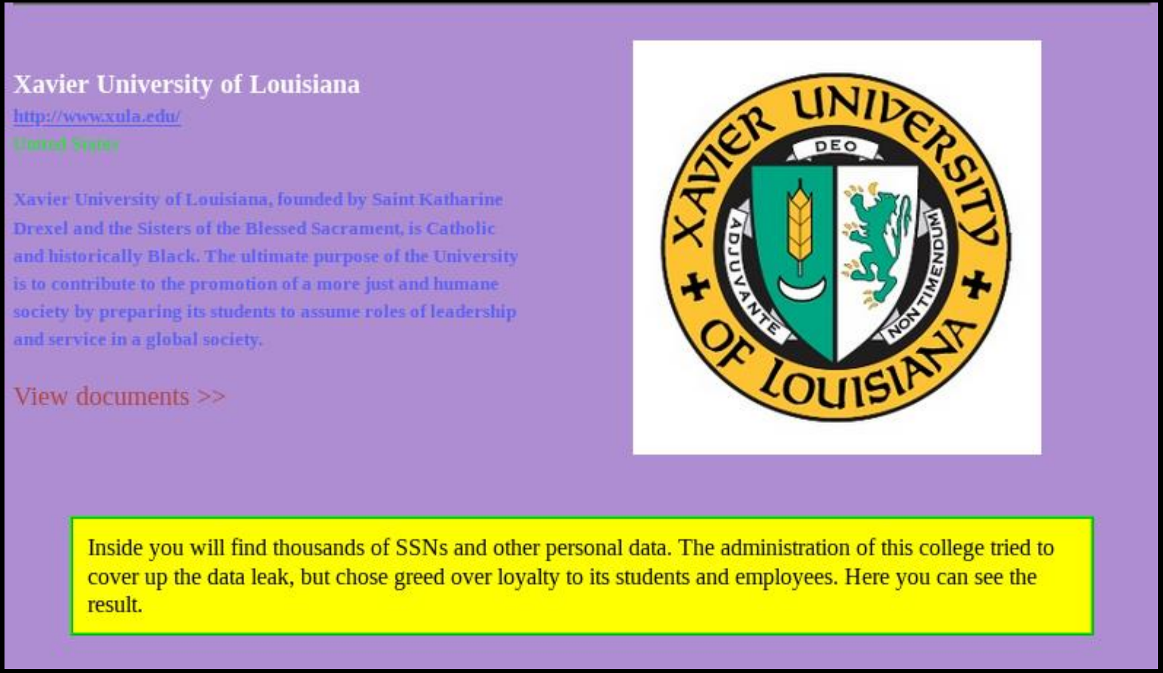
What do you do if the law says that someone can't pay you? Does that matter? What happens if the customer doesn't respond?
-We don't care about laws. If someone doesn't pay or doesn't contact us, we will publish their documents.

Has Vice Society published all the data it took from "company name" or does Vice Society have additional data that still has not been published?
-We always publish everything.

Can you explain your decision to publish "company name" data?
--They didn't pay.

We DON'T answer questions like:
What country or region of the world are you from?
How old are you?
What vulns/cve do you use?

Can things get any worse?



Xavier University of Louisiana

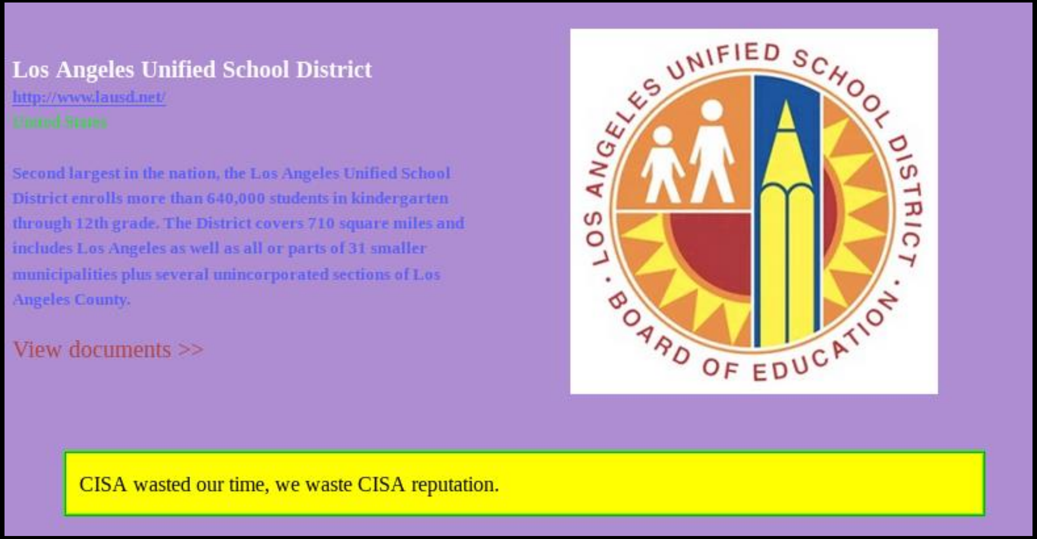
http://www.xula.edu/

United States

Xavier University of Louisiana, founded by Saint Katharine Drexel and the Sisters of the Blessed Sacrament, is Catholic and historically Black. The ultimate purpose of the University is to contribute to the promotion of a more just and humane society by preparing its students to assume roles of leadership and service in a global society.

View documents >>

Inside you will find thousands of SSNs and other personal data. The administration of this college tried to cover up the data leak, but chose greed over loyalty to its students and employees. Here you can see the result.



Los Angeles Unified School District

http://www.lausd.net/

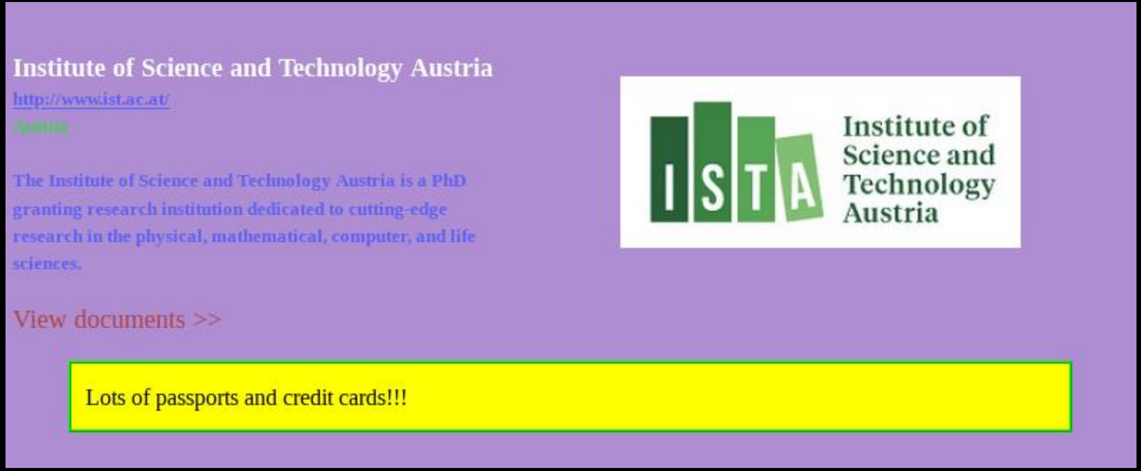
United States

Second largest in the nation, the Los Angeles Unified School District enrolls more than 640,000 students in kindergarten through 12th grade. The District covers 710 square miles and includes Los Angeles as well as all or parts of 31 smaller municipalities plus several unincorporated sections of Los Angeles County.

View documents >>

CISA wasted our time, we waste CISA reputation.

LOS ANGELES UNIFIED SCHOOL DISTRICT
BOARD OF EDUCATION



Institute of Science and Technology Austria

http://www.ist.ac.at/

Austria

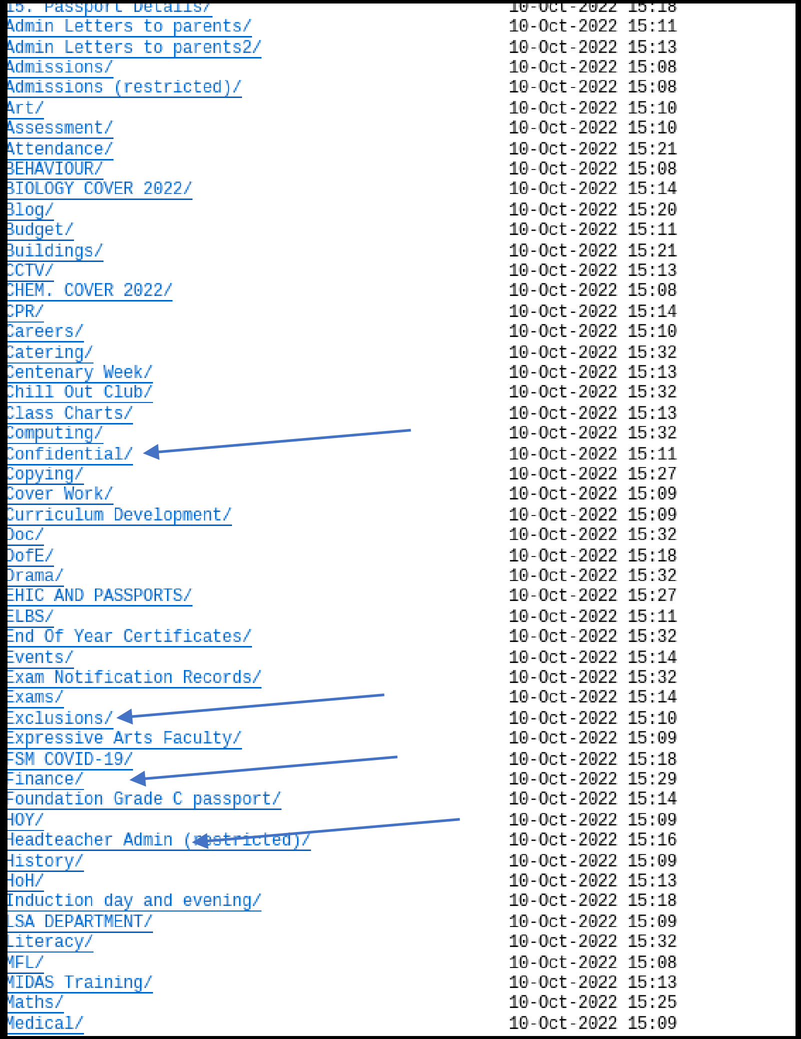
The Institute of Science and Technology Austria is a PhD granting research institution dedicated to cutting-edge research in the physical, mathematical, computer, and life sciences.

View documents >>

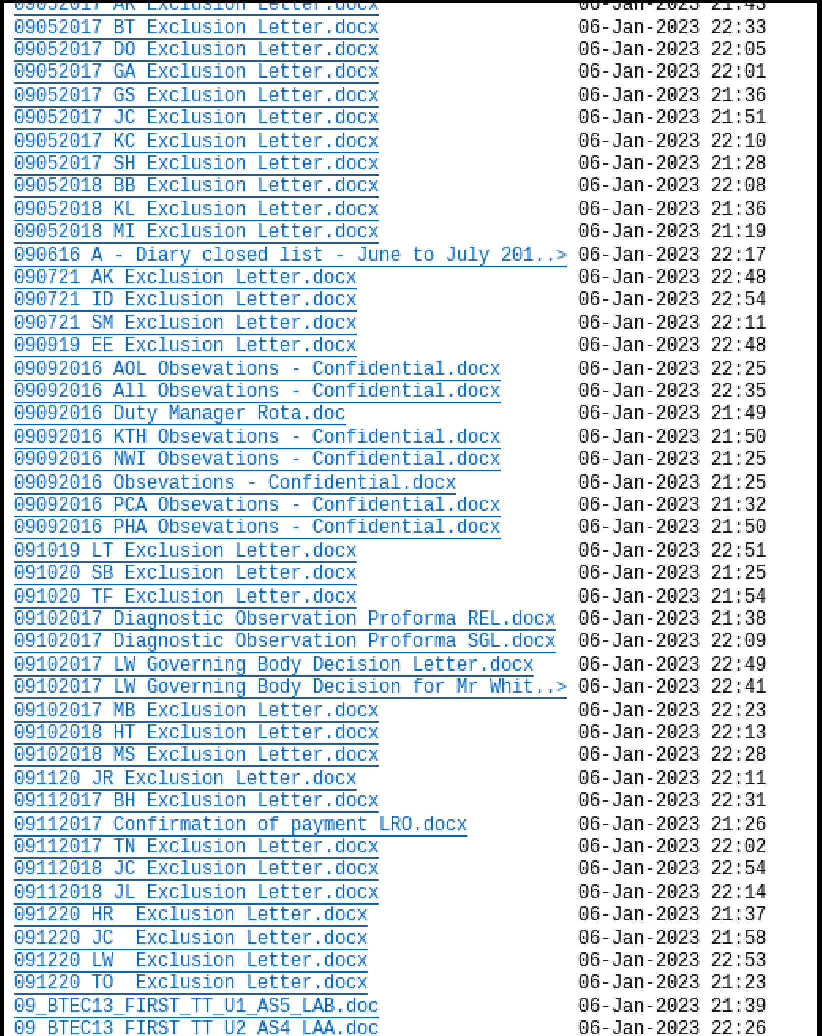
Lots of passports and credit cards!!!

ISTA
Institute of Science and Technology Austria

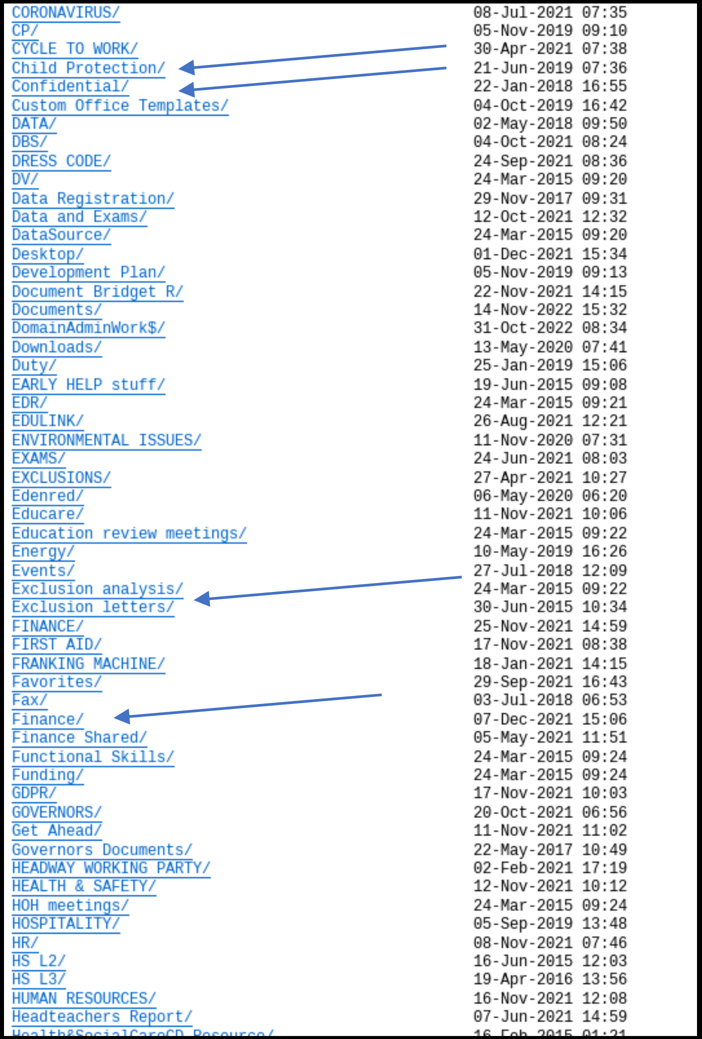
Can things get any worse?



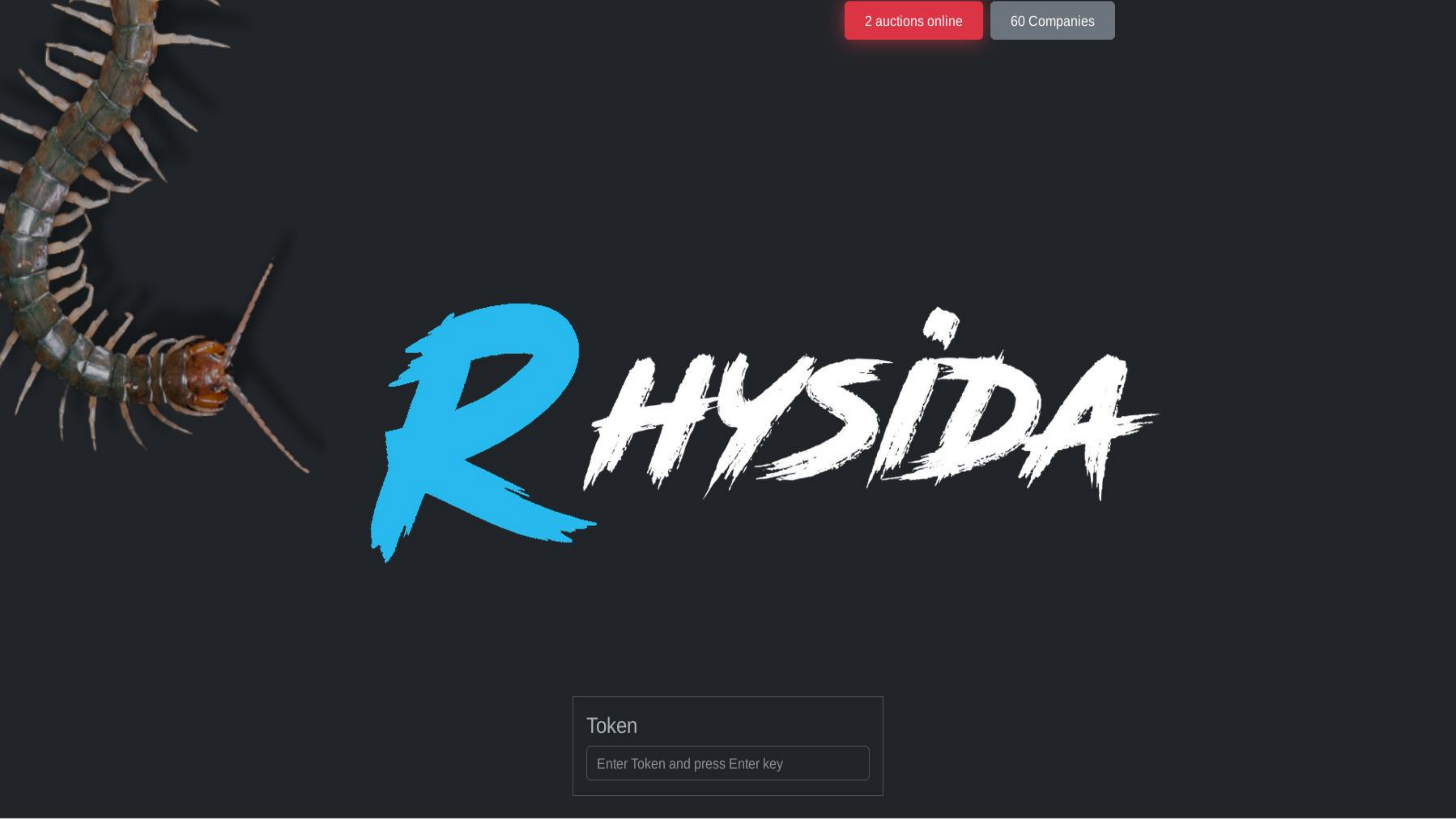
```
I5. Passport Details/                               10-Oct-2022 15:18
Admin Letters to parents/                           10-Oct-2022 15:11
Admin Letters to parents2/                          10-Oct-2022 15:13
Admissions/                                         10-Oct-2022 15:08
Admissions (restricted)/                            10-Oct-2022 15:08
Art/                                                10-Oct-2022 15:10
Assessment/                                         10-Oct-2022 15:10
Attendance/                                         10-Oct-2022 15:21
BEHAVIOUR/                                          10-Oct-2022 15:08
BIOLOGY COVER 2022/                                 10-Oct-2022 15:14
Blog/                                               10-Oct-2022 15:20
Budget/                                             10-Oct-2022 15:11
Buildings/                                          10-Oct-2022 15:21
CCTV/                                               10-Oct-2022 15:13
CHEM. COVER 2022/                                   10-Oct-2022 15:08
CPR/                                                10-Oct-2022 15:14
Careers/                                            10-Oct-2022 15:10
Catering/                                           10-Oct-2022 15:32
Centenary Week/                                     10-Oct-2022 15:13
Chill Out Club/                                     10-Oct-2022 15:32
Class Charts/                                       10-Oct-2022 15:13
Computing/                                          10-Oct-2022 15:32
Confidential/                                       10-Oct-2022 15:11
Copying/                                            10-Oct-2022 15:27
Cover Work/                                         10-Oct-2022 15:09
Curriculum Development/                             10-Oct-2022 15:09
Doc/                                                10-Oct-2022 15:32
DofE/                                               10-Oct-2022 15:18
Drama/                                              10-Oct-2022 15:32
EHIC AND PASSPORTS/                                 10-Oct-2022 15:27
ELBS/                                               10-Oct-2022 15:11
End Of Year Certificates/                           10-Oct-2022 15:32
Events/                                             10-Oct-2022 15:14
Exam Notification Records/                          10-Oct-2022 15:32
Exams/                                              10-Oct-2022 15:14
Exclusions/                                         10-Oct-2022 15:10
Expressive Arts Faculty/                            10-Oct-2022 15:09
FSM COVID-19/                                       10-Oct-2022 15:18
Finance/                                            10-Oct-2022 15:29
Foundation Grade C passport/                        10-Oct-2022 15:14
HOY/                                                10-Oct-2022 15:09
Headteacher Admin (restricted)/                     10-Oct-2022 15:16
History/                                            10-Oct-2022 15:09
HoH/                                                10-Oct-2022 15:13
Induction day and evening/                          10-Oct-2022 15:18
LSA DEPARTMENT/                                     10-Oct-2022 15:09
Literacy/                                           10-Oct-2022 15:32
MFL/                                                10-Oct-2022 15:08
MIDAS Training/                                     10-Oct-2022 15:13
Maths/                                              10-Oct-2022 15:25
Medical/                                            10-Oct-2022 15:09
```

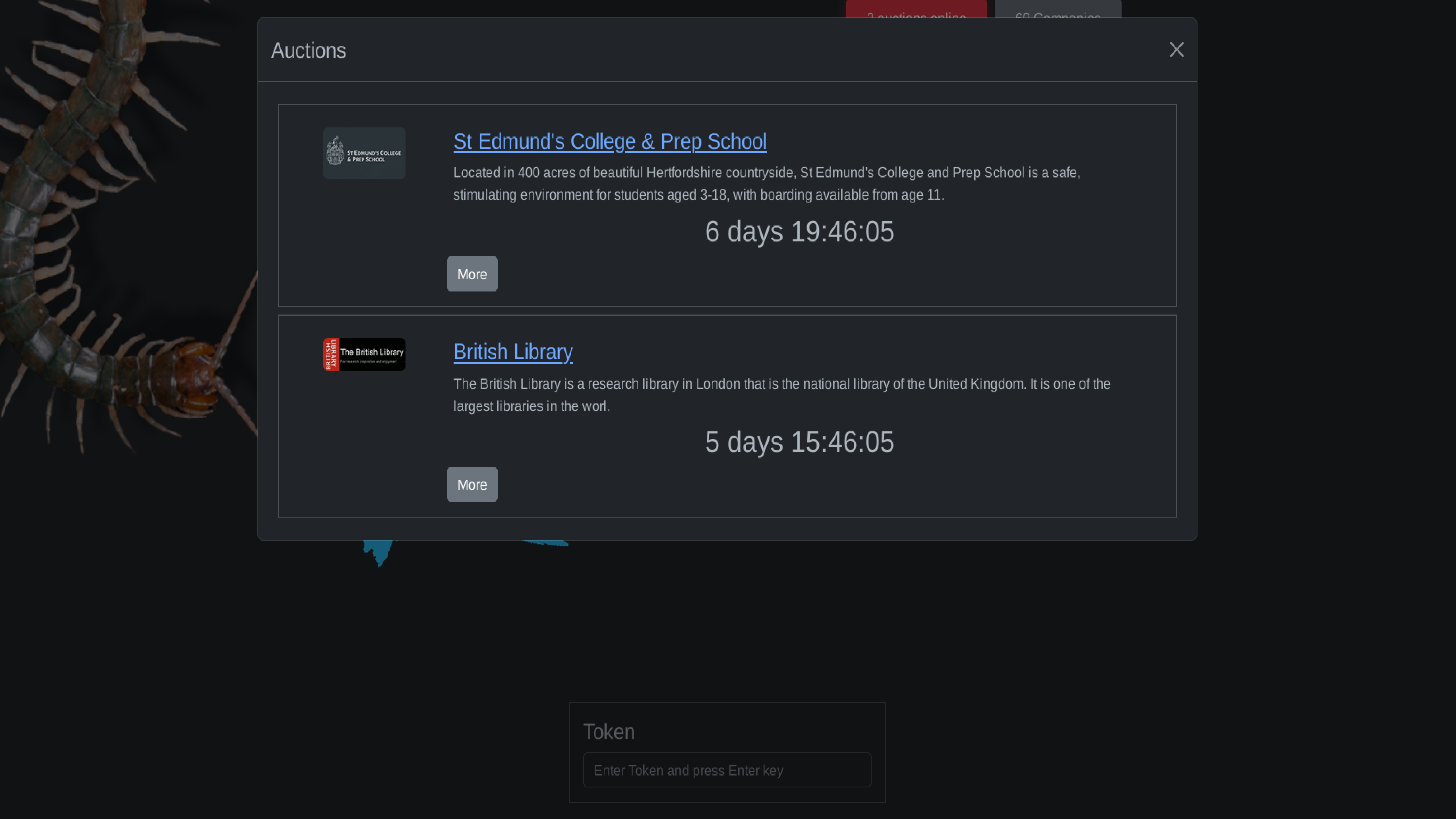


```
09052017 AK Exclusion Letter.docx                   06-Jan-2023 21:45
09052017 BT Exclusion Letter.docx                   06-Jan-2023 22:33
09052017 DO Exclusion Letter.docx                   06-Jan-2023 22:05
09052017 GA Exclusion Letter.docx                   06-Jan-2023 22:01
09052017 GS Exclusion Letter.docx                   06-Jan-2023 21:36
09052017 JC Exclusion Letter.docx                   06-Jan-2023 21:51
09052017 KC Exclusion Letter.docx                   06-Jan-2023 22:10
09052017 SH Exclusion Letter.docx                   06-Jan-2023 21:28
09052018 BB Exclusion Letter.docx                   06-Jan-2023 22:08
09052018 KL Exclusion Letter.docx                   06-Jan-2023 21:36
09052018 MI Exclusion Letter.docx                   06-Jan-2023 21:19
090616 A - Diary closed list - June to July 201..>  06-Jan-2023 22:17
090721 AK Exclusion Letter.docx                     06-Jan-2023 22:48
090721 ID Exclusion Letter.docx                     06-Jan-2023 22:54
090721 SM Exclusion Letter.docx                     06-Jan-2023 22:11
090919 EE Exclusion Letter.docx                     06-Jan-2023 22:48
09092016 AOL Obsevations - Confidential.docx        06-Jan-2023 22:25
09092016 All Obsevations - Confidential.docx        06-Jan-2023 22:35
09092016 Duty Manager Rota.doc                      06-Jan-2023 21:49
09092016 KTH Obsevations - Confidential.docx        06-Jan-2023 21:50
09092016 NWI Obsevations - Confidential.docx        06-Jan-2023 21:25
09092016 Obsevations - Confidential.docx            06-Jan-2023 21:25
09092016 PCA Obsevations - Confidential.docx        06-Jan-2023 21:32
09092016 PHA Obsevations - Confidential.docx        06-Jan-2023 21:50
091019 LT Exclusion Letter.docx                     06-Jan-2023 22:51
091020 SB Exclusion Letter.docx                     06-Jan-2023 21:25
091020 TF Exclusion Letter.docx                     06-Jan-2023 21:54
09102017 Diagnostic Observation Proforma REL.docx   06-Jan-2023 21:38
09102017 Diagnostic Observation Proforma SGL.docx   06-Jan-2023 22:09
09102017 LW Governing Body Decision Letter.docx     06-Jan-2023 22:49
09102017 LW Governing Body Decision for Mr Whit..>  06-Jan-2023 22:41
09102017 MB Exclusion Letter.docx                   06-Jan-2023 22:23
09102018 HT Exclusion Letter.docx                   06-Jan-2023 22:13
09102018 MS Exclusion Letter.docx                   06-Jan-2023 22:28
091120 JR Exclusion Letter.docx                     06-Jan-2023 22:11
09112017 BH Exclusion Letter.docx                   06-Jan-2023 22:31
09112017 Confirmation of payment LRO.docx           06-Jan-2023 21:26
09112017 TN Exclusion Letter.docx                   06-Jan-2023 22:02
09112018 JC Exclusion Letter.docx                   06-Jan-2023 22:54
09112018 JL Exclusion Letter.docx                   06-Jan-2023 22:14
091220 HR  Exclusion Letter.docx                    06-Jan-2023 21:37
091220 JC  Exclusion Letter.docx                    06-Jan-2023 21:58
091220 LW  Exclusion Letter.docx                    06-Jan-2023 22:53
091220 TO  Exclusion Letter.docx                    06-Jan-2023 21:23
09_BTEC13_FIRST_TT_U1_AS5_LAB.doc                   06-Jan-2023 21:39
09_BTEC13_FIRST_TT_U2_AS4_LAA.doc                   06-Jan-2023 22:26
```



```
CORONAVIRUS/                                        08-Jul-2021 07:35
CP/                                                 05-Nov-2019 09:10
CYCLE TO WORK/                                      30-Apr-2021 07:38
Child Protection/                                   21-Jun-2019 07:36
Confidential/                                       22-Jan-2018 16:55
Custom Office Templates/                            04-Oct-2019 16:42
DATA/                                               02-May-2018 09:50
DBS/                                                04-Oct-2021 08:24
DRESS CODE/                                         24-Sep-2021 08:36
DV/                                                 24-Mar-2015 09:20
Data Registration/                                  29-Nov-2017 09:31
Data and Exams/                                     12-Oct-2021 12:32
DataSource/                                         24-Mar-2015 09:20
Desktop/                                            01-Dec-2021 15:34
Development Plan/                                   05-Nov-2019 09:13
Document Bridget R/                                 22-Nov-2021 14:15
Documents/                                          14-Nov-2022 15:32
DomainAdminWork$/                                   31-Oct-2022 08:34
Downloads/                                          13-May-2020 07:41
Duty/                                               25-Jan-2019 15:06
EARLY HELP stuff/                                   19-Jun-2015 09:08
EDR/                                                24-Mar-2015 09:21
EDULINK/                                            26-Aug-2021 12:21
ENVIRONMENTAL ISSUES/                               11-Nov-2020 07:31
EXAMS/                                              24-Jun-2021 08:03
EXCLUSIONS/                                         27-Apr-2021 10:27
Edenred/                                            06-May-2020 06:20
Educare/                                            11-Nov-2021 10:06
Education review meetings/                          24-Mar-2015 09:22
Energy/                                             10-May-2019 16:26
Events/                                             27-Jul-2018 12:09
Exclusion analysis/                                 24-Mar-2015 09:22
Exclusion letters/                                  30-Jun-2015 10:34
FINANCE/                                            25-Nov-2021 14:59
FIRST AID/                                          17-Nov-2021 08:38
FRANKING MACHINE/                                   18-Jan-2021 14:15
Favorites/                                          29-Sep-2021 16:43
Fax/                                                03-Jul-2018 06:53
Finance/                                            07-Dec-2021 15:06
Finance Shared/                                     05-May-2021 11:51
Functional Skills/                                  24-Mar-2015 09:24
Funding/                                            24-Mar-2015 09:24
GDPR/                                               17-Nov-2021 10:03
GOVERNORS/                                          20-Oct-2021 06:56
Get Ahead/                                          11-Nov-2021 11:02
Governors Documents/                                22-May-2017 10:49
HEADWAY WORKING PARTY/                              02-Feb-2021 17:19
HEALTH & SAFETY/                                    12-Nov-2021 10:12
HOH meetings/                                       24-Mar-2015 09:24
HOSPITALITY/                                        05-Sep-2019 13:48
HR/                                                 08-Nov-2021 07:46
HS L2/                                              16-Jun-2015 12:03
HS L3/                                              19-Apr-2016 13:56
HUMAN RESOURCES/                                    16-Nov-2021 12:08
Headteachers Report/                                07-Jun-2021 14:59
Health&SocialCareCD Resource/                       16-Feb-2015 01:21
```


2 auctions online
60 Companies
RHYSIDA
Token
Enter Token and press Enter key



Auctions

St Edmund's College & Prep School

Located in 400 acres of beautiful Hertfordshire countryside, St Edmund's College and Prep School is a safe, stimulating environment for students aged 3-18, with boarding available from age 11.

6 days 19:46:05

British Library

The British Library is a research library in London that is the national library of the United Kingdom. It is one of the largest libraries in the worl.

5 days 15:46:05

Token

Ransomware groups

- perhaps the biggest source of raw data for further attacks is stolen/exfiltrated data
  - student/children's data has a value in terms of clean credit history, as they reach credit card age – passport scans are gold.
  - also used in people smuggling!
  - the buying and selling of data in bulk happens, as well as the development of *data lakes* for data matching – *probably using the same tools as you on Azure/AWS/GCP?*
- interconnected point experts, subcontractors and affiliates, escrow and payment arrangements via crypto coin – *(analysis of crypto coin has been useful here)*

Soft yet powerful defense: conferences and events like this

- early sharing of attack techniques used with others schools
- early sharing of attacks / bad day info

Relentless: Scanning of your external stuff:

The reality of the matter, in the ransomware ecosystem, is initial access brokering is cheap and affordable, it is a worthwhile investment for ransomware affiliates to establish a good relationship with an initial access broker.

There is an initial access broker who will sell you roughly 1,000,000 misconfigured VPN's for $1,500.

These 'misconfigured' VPNs typically will be companies which have accidentally set a VPN user login to something like 'test' as the username AND password.

Although this may sound absurd, or unlikely, these are extremely common as organisations may simply overlook small errors. However, these misconfigured VPNs are not curated.

Ransomware affiliates might have to spend weeks, or months, sorting through the list determining which companies discovered have:

- Money
- Do not violate the rules of the ransomware group
- Have insufficient security posture
- Are outside with CIS (ex-soviet countries).

Regarding targets, another aspect often overlooked

Ransomware operators often do not understand the culture or targets they have identified.

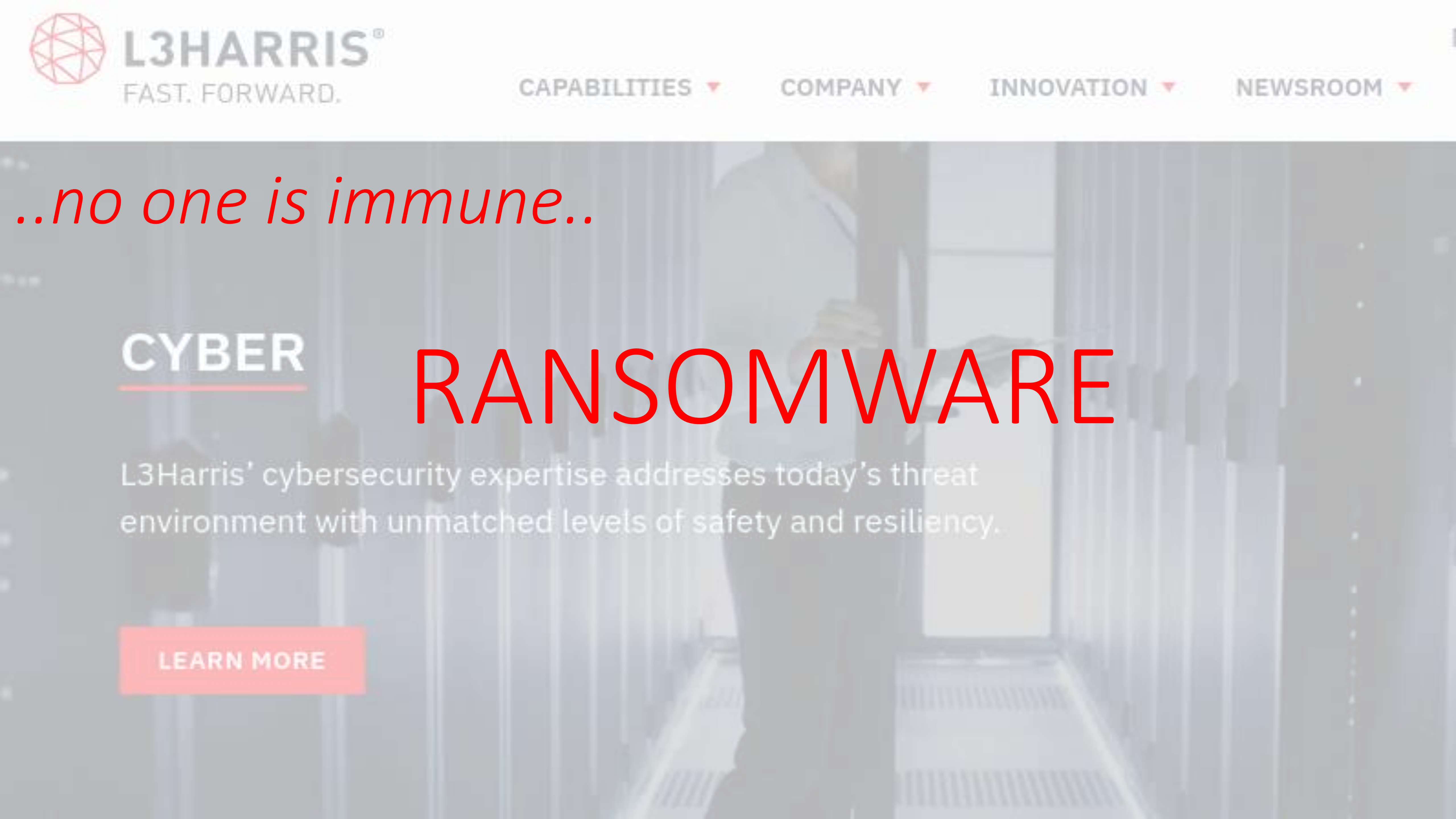
For example, we have witnessed these ransomware groups target school systems, failing to understand how money is allocated for schools.

They mistakenly believe tax-funded schools are ripe with cash and simply do not believe negotiators when they say the victim doesn't have the money. They rely on publicly available information (often wrong information) from places like Wikipedia or ZoomInfo. They see big numbers and believe that this is the profit margins.

NOTE: Every ransomware affiliate will seek different avenues of gaining access.

..no one is immune..

RANSOMWARE



CYBER

L3Harris' cybersecurity expertise addresses today's threat environment with unmatched levels of safety and resiliency.

“*we, Knapweed* ” share know how on detection

Script Block Logging must be enabled in Windows for all script blocks to be logged.

- Then implement the YARA rule provided in this article within your security systems.
- Enable PowerShell Module and Script Block Logging in PowerShell.
- Check Windows Event Logs Event IDs 400, 600, 800, 4103 and 4104.
- Search for the script’s function names in 4104 events:
    - Work($disk) - Show($name) - CreateJobLocal($folders) - fill([string]$filename)

Monitor for command lines that include the following: powershell.exe - ExecutionPolicy Bypass - file \\[internal_ip_address]\s$\w1.ps1

- Look for HTTP POST events to /upload endpoints on unknown remote HTTP servers.
- Look for HTTP activity direct to external IP addresses, if you have this visibility.
- Detect spikes in network traffic:

Do you have a network baseline? Use it to determine when network traffic from a set of hosts far exceeds the baseline. Do you have a SIEM, SOAR or log aggregation utility that will allow you to alert on HTTP POST sizes?

- Perhaps look for when a count of POST events to a given site – especially an IP address – exceeds a baseline. Also look into alerting for when a POST event has a request size over a given threshold.
- For example, you might want an alert when any POST event has a file size > 10 MB. This will require tuning and insight into what is normal in your environment.
- Look into network traffic spikes generated by non-expected accounts. For example, should your Domain Admin, Enterprise Admin or general service accounts be making large POST requests? Is this something for which you can generate alerts?

Project Knapweed "basics" of protecting your organistation:

1. If you only use a username and password to access school systems from beyond the school network you are at a **massive risk**.
2. If your IT systems are not fully patched for critical updates within 14 days of their release you are at **massive risk**.
3. Strongly consider adding a DMARC DNS record to your email system so your email is trusted and less likely to be used to attack others.
4. Consider doing Cyber Essentials (CE) as a base line for cyber security standards
5. Consider a Security Information Event Management system (SIEM) or Security Operations Centre (SOC) – (maybe best at Trust or LEA level).

You can do a lot in an inbox… £4m, *or just an entry point to your network/data?*

thank you for hearing what I have to say,
questions?

more on dark web, ransomware and email!
https://ctag.gov.uk

C-TAG
Cyber - Technical Advisory Group
Coordinating Local Public Services Cyber

Part 3

Prepare for Ransomware

Rob Tillman

Hampshire County Council

Proactive Recommendations – Cyber Security Frameworks – NCSC Large Organisations

This framework is aimed at larger organisations. It has 10 areas which should be reviewed to improve your Cyber Security posture.

Risk management	Engagement and training	Asset management	Architecture and configuration	Vulnerability management
Identity and access management	Data security	Logging and monitoring	Incident management	Supply chain security

Proactive Recommendations – Cyber Security Frameworks – NCSC Smaller Organisations

Backup your data	Protect from Malware	Keep all your devices safe	Password protect data	Avoid phishing emails
• Know what you need to backup. • Keep backups separate to the computer systems. • Consider cloud backup location • Read NSCS 3-2-1 guidance. • Make backups part of everyday operation.	• Install AV • Stop staff downloading unauthorised software. • Patch everything, keep it up to date. • Control USB • Enable firewalls	• Password protect all devices. • Make sure you can remote wipe devices. • Keep apps and devices patched. • Don't connect to unknown networks	• Turn on passwords wherever possible. • Use Multi Factor Authentication. • Avoid predictable passwords • Change all default passwords. • Password managers.	• Restrict accounts • Report all attacks • Check your digital footprint • Stop, Think, Breath (user training)

Hampshire County Council

Hampshire Services HIAS SCHOOL IMPROVEMENT

Proactive Recommendations

Prepare

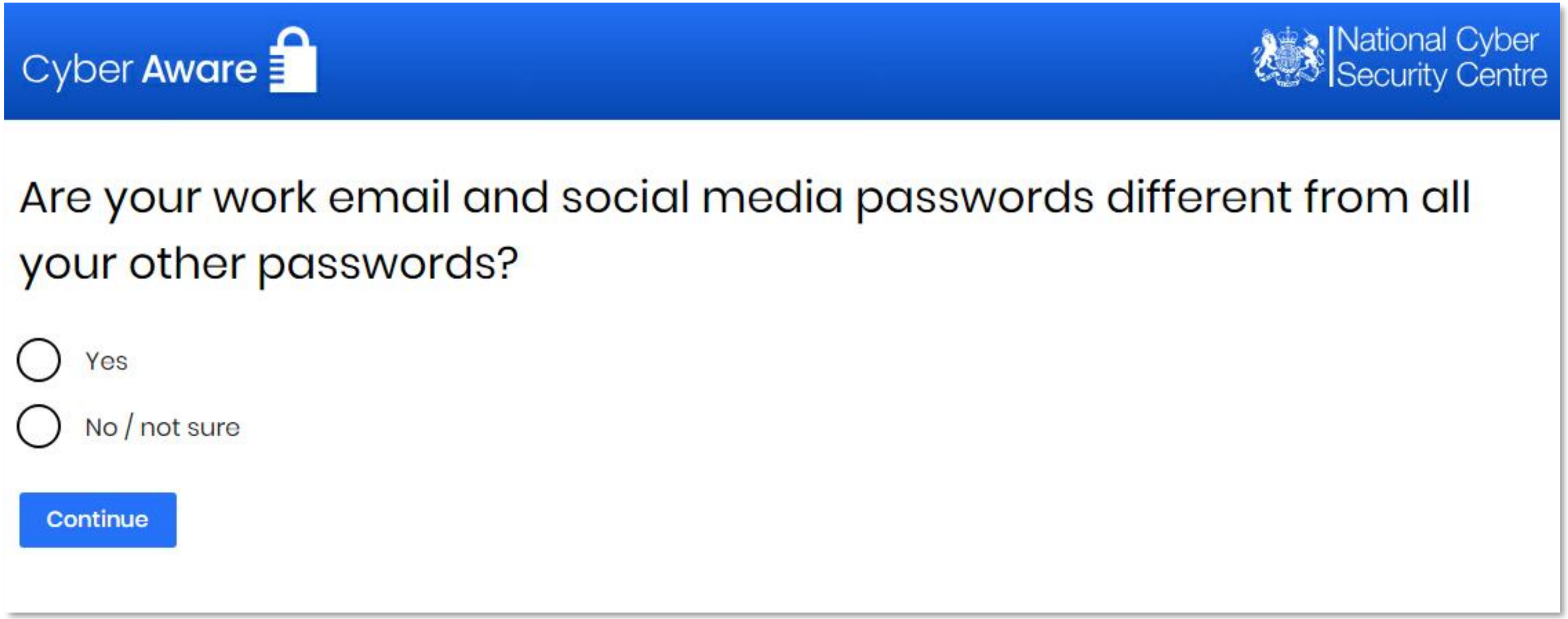
- Baseline your school
- Response plan and business continuity plans
- Staff Engagement and training

Technical Controls

- Backups
- Prevent delivery
- Prevent it spreading
- Monitor and Alert

Proactive Recommendations - Baseline Your Cyber Security Position

The National Cyber Security Centre (NCSC) offer a cyber action plan on their website - https://www.ncsc.gov.uk/cyberaware/actionplan



Are your work email and social media passwords different from all your other passwords?

○ Yes

○ No / not sure

Proactive Recommendations - Prepare – Business Continuity Plan

Key aspects (business continuity IT related)

- Know what data you have. (for example what data do you hold, on whom)

- What are your business-critical systems. (where are they hosted? (SIMS, Finance) How do you access those systems?)

- Know what do you need available to run the school. (What business processes and associated IT systems you are needed to run the school. Are there non-IT options to run those processes? What will you do if IT is unavailable?)

- Know who your stakeholders are. (Have an offline list of useful contacts. This should include emergency contacts such as NCSC, Action Fraud and any IT response partner you might need to engage.)

- Know what your endpoints are. (this should include any system used to access your data. Tablets, PC's laptops, servers, phones.)

- Know what is on your network. (often overlooked things like building management systems, specialist printers and tills all need to be considered.)

- Know who you connect to and what data they hold on your behalf. (Supplier chain vulnerabilities are becoming increasingly prevalent, so it might not be your systems that are compromised directly!)

Proactive Recommendations - Prepare – Response Plan.

Key aspects (response plan)

- Agree pre-approved actions. (Time is critical during a response. If you are happy for the IT team to turn off, web servers, or the admin and curriculum networks in event of ransomware, pre-agree that!)
- Make decisions. (document them e.g. Does your response include evidence protection or just recovery steps? It is incredibly difficult to hold ransomware threat actors to account, protection of evidence is probably not likely to be beneficial so you may want to focus on speedy recovery.)
- Know how to isolate your network. (Internet access, Partner VPN's, other schools)
- Know how to turn off access to systems. (both on-premises and cloud solutions)
- Know how to secure your offline backups.
- Know who you need to talk to. (the main stakeholders, but also have statements prepared for the inevitable press questions.)
- Have pre canned statements

Proactive Recommendations – Prepare – Staff Engagement And Training

Probably one of the key areas for cyber security is staff!

- You will never be able to cover every single technical scenario with training and advice.
  - As we cannot cover everything, psychology becomes as important as technology.
- Staff are your first line of defence when it comes to cyber security, they are also your last line and possibly the weakest link.
- Undertake email phishing training, there are a lot of free options out there to do this.
  - When doing this, ensure you give support to staff who “fail”.
- Get staff thinking about their digital footprint (e.g. devices, USB sticks, email accounts, passwords, social media etc.).
- Cultivate a culture of shared responsibility.
- Promote open discussions.

Proactive Recommendations – Prepare – Staff Engagement And Training

Some unpopular recommendations:

- Don’t allow staff to use their work email for personal purposes.
- Don’t allow staff to use social media unless it is directly for their role.
- Don’t allow staff to use web mail, unless it is directly related to their role.
- Limit internet browsing in general (you’ll already be doing this).

Adversary Tactics

- Deception
- Emotional Stress
- Time Pressure
- Isolation
- Greed
- Exploitation

Stay Safe - Stop. Breathe. Think.

We protect each other – don't act alone.

Talk to your social circle, work circle, official support channels – **especially** if you have/think you have been tricked

Trust but Verify

Use another method to confirm legitimacy

Question it

Why have I received this? What's its purpose?

Look for warning signs

"Trust your feelings"

Use information you've sourced yourself

URLs, phone numbers, email addresses etc

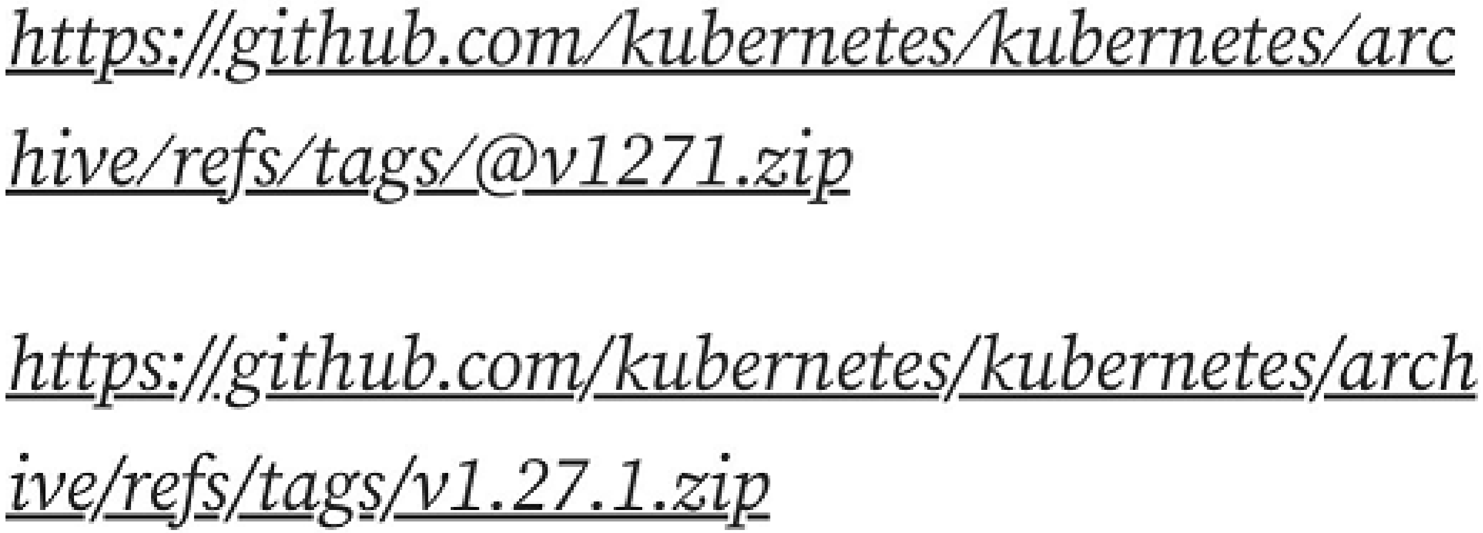
You are in control

The burden of proof is on it/them. Challenge, stall, question.

Don't be afraid to say

Brain Teaser

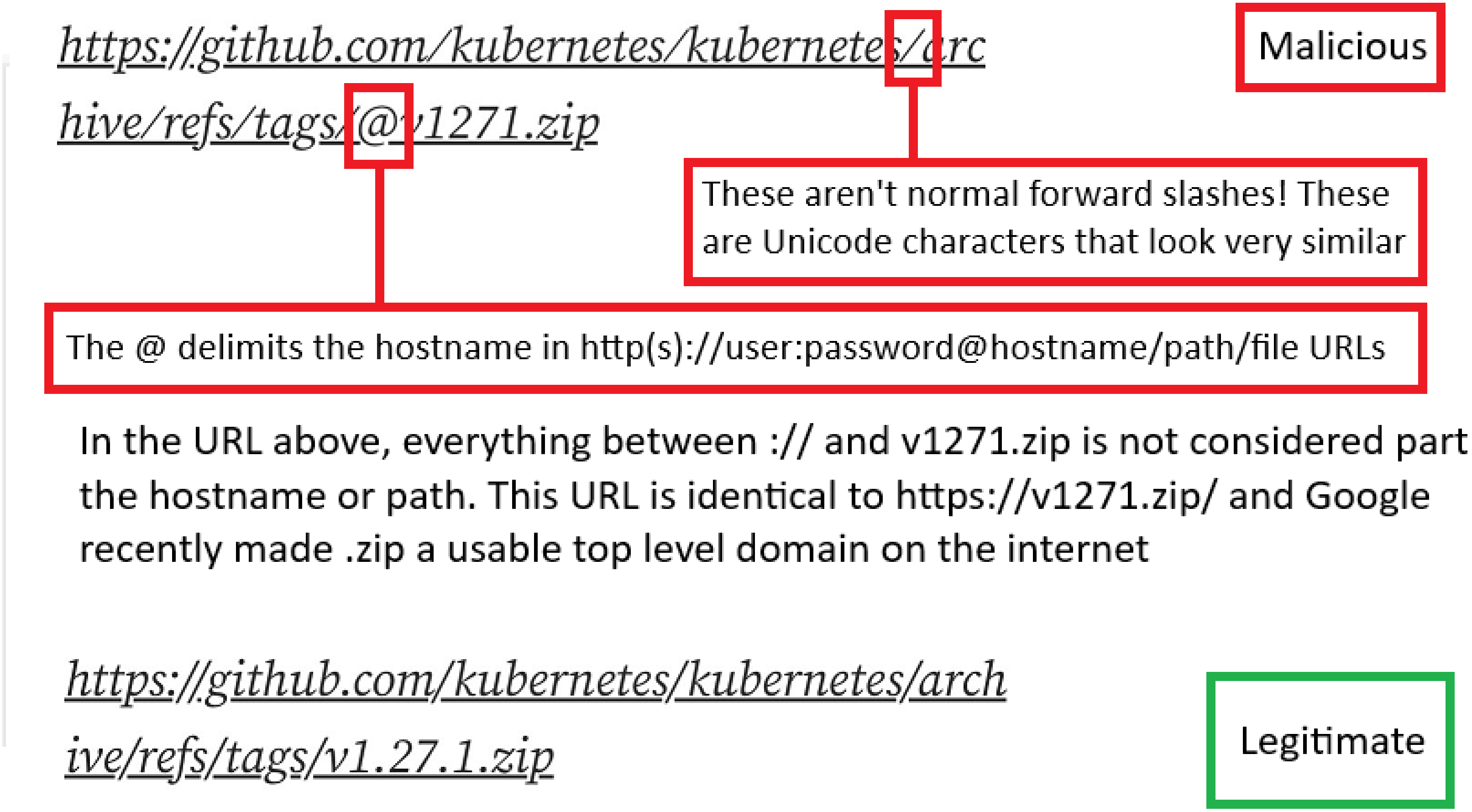
1. One of these URLs is legitimate and downloads a zip file, the other is malicious and downloads evil.exe – which one is which?
2. Why does the malicious one download evil.exe?



https://github.com∕kubernetes∕kubernetes∕archive∕refs∕tags∕@v1271.zip

https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip

Answer



https://github.com/kubernetes/kubernetes/archive/refs/tags/@v1271.zip

Malicious

These aren't normal forward slashes! These are Unicode characters that look very similar

The @ delimits the hostname in http(s)://user:password@hostname/path/file URLs

In the URL above, everything between :// and v1271.zip is not considered part of the hostname or path. This URL is identical to https://v1271.zip/ and Google recently made .zip a usable top level domain on the internet

https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip

Legitimate

Proactive Recommendations - Technical Controls - Backups

Aspects to consider for backups.

- Identify all your key data and systems.
- Have a regular backup schedule, ideally nightly.
- Immutable backups are becoming essential!
- Consider backups of cloud services (OneDrive, Exchange Online, SharePoint)
- Considering backing up to the cloud, or back up to another school.
- Test your backups on a regular basis.
- Verify your backups.

NCSC recommends a 3-2-1 backup strategy:

- **3** copies of data
- **2** locations
- **1** offline or protected

Proactive Recommendations - Technical controls - Prevent delivery – User Aspects

The simple things

- All accounts should have strong passwords. (Good practice - three random words, 15 characters, complex)
- Two factor authentication should be enforced on all accounts.
- Avoid password reuse. (do not use work passwords for any personal use)

Least privilege principle

- User accounts should only be granted the privileges they need to do their job.
- Separate user accounts for high privileged functions and standard user activities.

Proactive Recommendations Technical controls - Prevent delivery - IT Team

Secure By Design (Layers of protection)

- Segment your network.
- Implement patch management and lifecycle processes for new systems / software.
- Limit and control external connectivity, especially RDP services and remote assistance tools.
- When implementing solutions which leave the School environment ensure there are remote wipe capabilities.
- Implement multi factor authentication for all systems if used over internet.

Proactive Recommendations Technical controls - Prevent delivery - IT Team

- Enable all available email protections you have available.
- Limit web viewing (No access to social media for example).
- Implement NCSC PDNS as soon as it becomes available.
- Change default passwords.
- Provide password management capability, use it.
- Monitor your estate – external and internal scans

Proactive Recommendations - Technical Controls - Prevent It Spreading

Endpoint protections

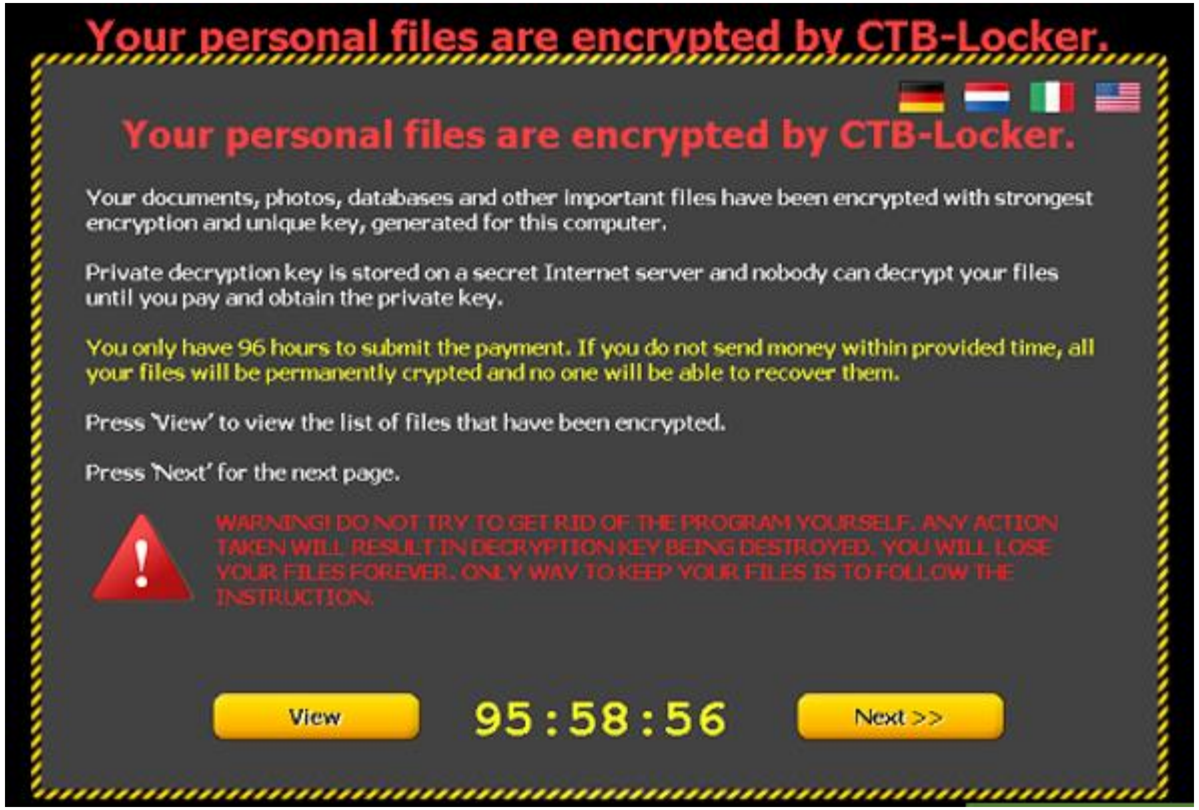
Patch Operating systems regularly.	Physically protect access to devices.
Patch software regularly.	Enable and configure local device firewalls.
Ensure anti-virus is enabled.	Encryption to protect in event of theft.
Disabled USB storage.	Create allow lists for application that can be used.
Password protect devices.	Unpopular opinion - Standard users should not have local administrative rights on End Points.

Proactive Recommendations Technical Controls – Monitor and Alert

NCSC Early Warning (free for public sector)
Early Warning is a NCSC service designed to inform your organisation of potential cyber attacks on your network, as soon as possible. The service uses a variety of information feeds from the NCSC, trusted public, commercial and closed sources, which includes several privileged feeds which are not available elsewhere.

Security Information and Event Management (SIEM) solutions
SIEM solutions aggregate log data from all your devices and systems across the organisation. It undertakes analysis of the data and reports back threats so you can react to them. There are dozens of options on the market, with various services attached to them. Or you can opt for opensource versions.

Ransomware event



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

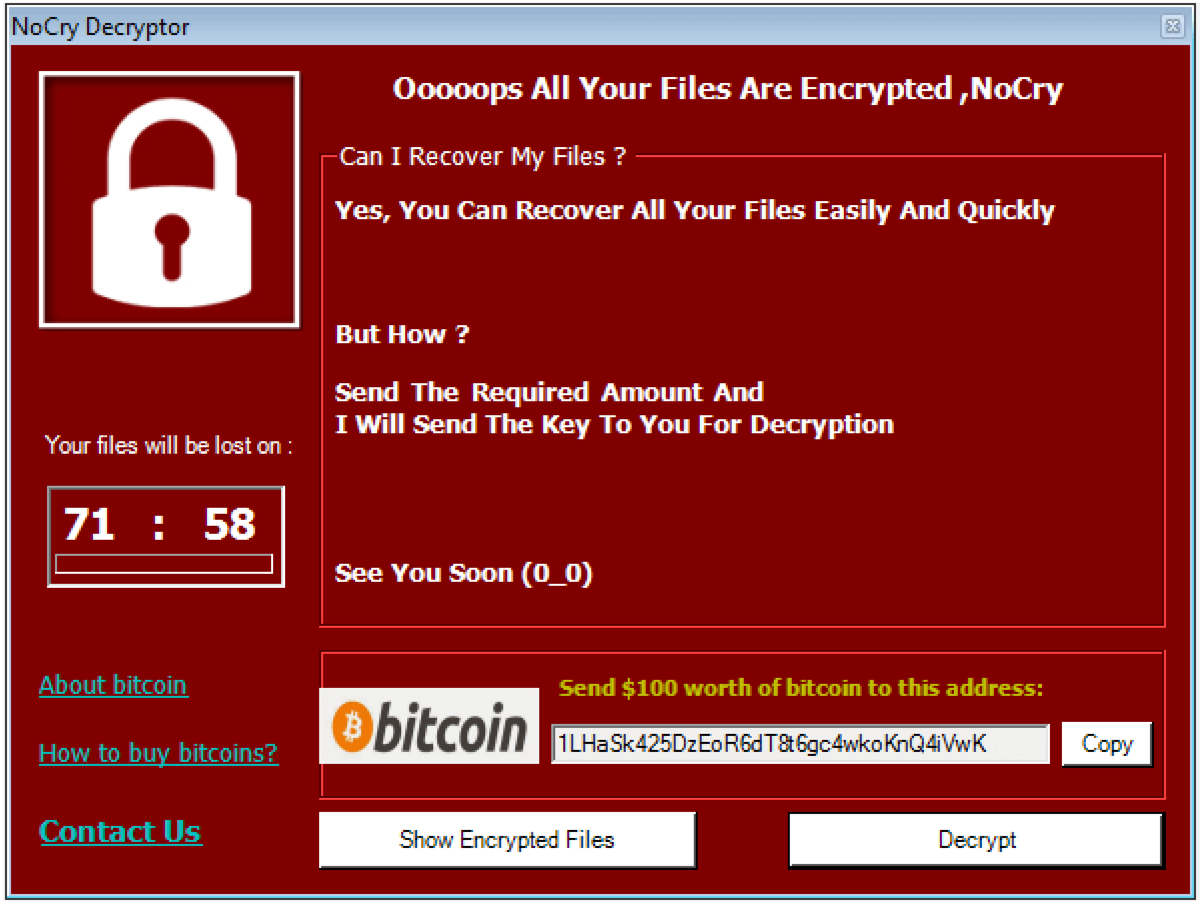
You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

95 : 58 : 56



NoCry Decryptor

Ooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

Yes, You Can Recover All Your Files Easily And Quickly

But How ?

Send The Required Amount And
I Will Send The Key To You For Decryption

See You Soon (0_0)

Your files will be lost on :

71 : 58

Send $100 worth of bitcoin to this address:

1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

What to do in worst case scenario - Should I pay the ransom?

Ransomware is a blackmail technique.

Law enforcement does not encourage, endorse nor condone the payment of ransom demands. If you do pay the ransom:

- There is no guarantee that you will get access to your data or computer
- Your computer will still be infected
- You will be paying criminal groups
- You're more likely to be targeted in future
- **They will still have a copy of your data**

For this reason, it is important that you always have a recent offline (protected) backup of your most important files and data.

https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/ico-and-ncsc-stand-together-against-ransomware-payments-being-made/

What to do in worst case scenario – Response - Invocation of plans

- Consider incident response specialists to assist.
- Ask for help. Talk to initiatives such as Project Knapweed.
- Evidence or Recovery
- Investigation, check for indicators of compromise
- Power everything down.

What to do in worst case scenario – Response - Investigation Common stumbling points

- Starting mitigation before investigation finishes.
- Touching adversary infrastructure.
- Pre-emptively block adversary infrastructure.
- Pre-emptively change credentials.
- Fail to collect log data which will identify route cause / entry point.
- Communicate across, or use systems on same compromised network.
- Treating symptoms, not the root cause.

What to do in worst case scenario – Response - Investigation

Answer the key questions – who, what, when, why.

Who undertook it?

- Where / How did they get in.

What did they do?

- Ransomware (what did they target, OS, user files, email?)
- Credential theft.
- Evidence of Backdoors.
- Scope of infiltration (e.g. admin, curriculum).

When did they do it?

- First indicator of compromise.
- First action against systems.
- Any virus alerts?

Why?

- Extracted data / extortion?
- Monetary / ransom.
- Malicious content on web site? (extremists)

What to do in worst case scenario – Response - Investigation

Answer the key questions – indicators of compromise

Commonality of infected systems
Subnet
Type of server
Domain
Operating System

Check for communication to command and control server
From servers
From devices
From network components

Checked for evidence of malicious applications
Bloodhound
AD Recon script
Rubeus
Responder
WebHunter
CrackMapExec

Check for remote management tools being active
AnyDesk
Atera Remote management
Ngrok.io
Remote manipulator system
Splashtop
Teamviewer

Check anti virus alerts
Time stamps if picked up
Services being stopped

What to do in worst case scenario – Response - Investigation

What did the threat actor get to
Domain controllers?
Data Servers?
Web Servers?
Authentication services?
Payment services?
Local server password cache (stepping stone to other devices / domain admin)

Checked for evidence of Account / AD modification
New users (domain or local)
Domain admin group changes / local admin group
Other privileged group changes

Check for evidence of any interaction with Azure Tenancies
New users
Global admin functions assignment
Other privileged roles

Check Network traffic
Out of the organisation? (exfiltration of data to drop box services? ftp/sftp)
Between impacted hosts?
To other hosts?

Check for automation
Any scheduled tasks created?
Any rules created for email accounts?

Plan for investigation
Specific evidence / areas of interest
How to ascertain timelines (IIS logs, event logs on compromised components)
Entry point user (phishing, macro content, malicious files, browser) or system (RDP, misconfiguration)
Account validation, what accounts used, compromised account / domain process

What to do in worst case scenario - Recovery

- Ensure the entry point is identified.

- Verify devices – hypervisors, laptops, PC’s.
- Verify Network components – are they AD linked? Isolated credentials.
- Verify with partners – did the infection hit them, are they clean?

- Rebuild – bare metal, level of compromise ascertained (is your firmware OK?)
- Creation of clean zone networks or processes.
- Restore – “good” verified backup data set, offsite (check against initial times of IOC’s)
- Ensure entry point is closed.
- Continued communication with stakeholders

- Check restored data
  - Virus scan it.
  - Check for unknown or unusual files or folder structures.
  - Are encrypted files still prevalent.

- Change every password in the school. The threat actor could well have taken copies of Active Directory to crack offline and come back.

Summary

Your checklist

Review

Review the privacy settings for your social media, professional networking sites and app accounts.

Know

Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check

Check your device is set to receive updates automatically.

Set

Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove

Remove any apps that have not been downloaded from official stores.

Check

Check that the password for your work account is unique.

Flag it

If it's not possible to follow security advice, process or policy - flag it to your IT team.

Summary

We have covered a lot of topics during the presentation. Here are some key take aways:

1. Make time for cyber security, it is a lot to deal with, break it down and spread it out.
2. Cyber security is everyone’s responsibility within the school, not just the IT staff.
3. Treat it as a continuous improvement programme, train your staff on a monthly basis.
4. Do the NCSC baseline work.
5. Your data is your crown jewels. **Back it up**, make it safe.
6. Use multi factor authentication on **everything** you can access over the internet.
7. Check that your suppliers are safeguarding your data.
8. Assume you will be attacked and have a plan.

Your feedback matters

Please scan the QR code to complete our online training evaluation form

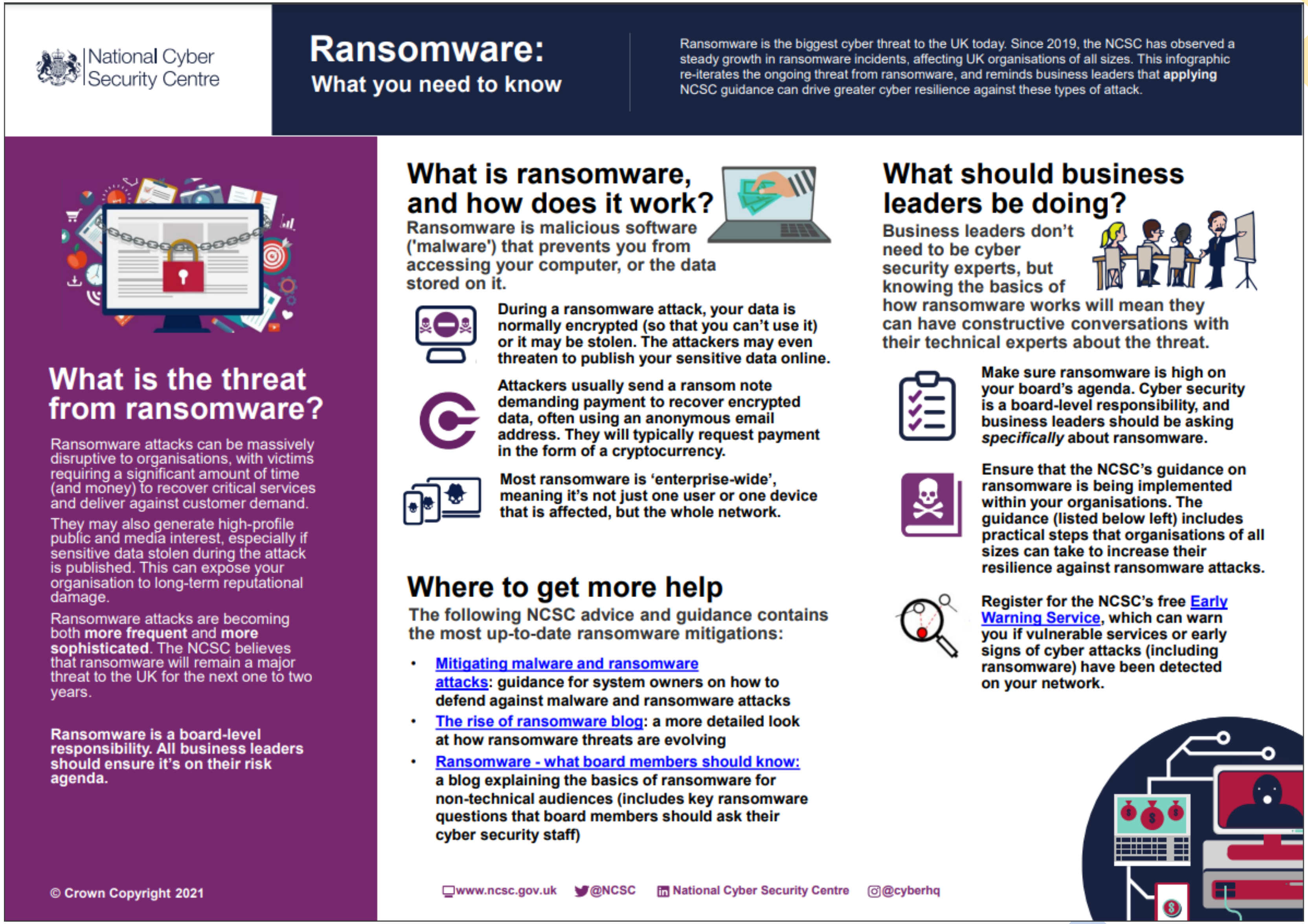
Or access the form using the URL below

https://forms.office.com/r/QE21XtDJ2r

Thank you!

Useful links slides

Hampshire
County Council



National Cyber Security Centre

Ransomware:

What you need to know

Ransomware is the biggest cyber threat to the UK today. Since 2019, the NCSC has observed a steady growth in ransomware incidents, affecting UK organisations of all sizes. This infographic re-iterates the ongoing threat from ransomware, and reminds business leaders that **applying** NCSC guidance can drive greater cyber resilience against these types of attack.

What is the threat from ransomware?

Ransomware attacks can be massively disruptive to organisations, with victims requiring a significant amount of time (and money) to recover critical services and deliver against customer demand.

They may also generate high-profile public and media interest, especially if sensitive data stolen during the attack is published. This can expose your organisation to long-term reputational damage.

Ransomware attacks are becoming both **more frequent** and **more sophisticated**. The NCSC believes that ransomware will remain a major threat to the UK for the next one to two years.

Ransomware is a board-level responsibility. All business leaders should ensure it's on their risk agenda.

What is ransomware, and how does it work?

Ransomware is malicious software ('malware') that prevents you from accessing your computer, or the data stored on it.

During a ransomware attack, your data is normally encrypted (so that you can't use it) or it may be stolen. The attackers may even threaten to publish your sensitive data online.

Attackers usually send a ransom note demanding payment to recover encrypted data, often using an anonymous email address. They will typically request payment in the form of a cryptocurrency.

Most ransomware is 'enterprise-wide', meaning it's not just one user or one device that is affected, but the whole network.

Where to get more help

The following NCSC advice and guidance contains the most up-to-date ransomware mitigations:

- Mitigating malware and ransomware attacks: guidance for system owners on how to defend against malware and ransomware attacks
- The rise of ransomware blog: a more detailed look at how ransomware threats are evolving
- Ransomware - what board members should know: a blog explaining the basics of ransomware for non-technical audiences (includes key ransomware questions that board members should ask their cyber security staff)

What should business leaders be doing?

Business leaders don't need to be cyber security experts, but knowing the basics of how ransomware works will mean they can have constructive conversations with their technical experts about the threat.

Make sure ransomware is high on your board's agenda. Cyber security is a board-level responsibility, and business leaders should be asking *specifically* about ransomware.

Ensure that the NCSC's guidance on ransomware is being implemented within your organisations. The guidance (listed below left) includes practical steps that organisations of all sizes can take to increase their resilience against ransomware attacks.

Register for the NCSC's free Early Warning Service, which can warn you if vulnerable services or early signs of cyber attacks (including ransomware) have been detected on your network.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Useful links

NCSC Guidance

https://www.ncsc.gov.uk
https://www.ncsc.gov.uk/cyberaware/actionplan
https://www.ncsc.gov.uk/collection/board-toolkit
https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf
https://www.ncsc.gov.uk/files/Ransomware_what_you_need_to_know.pdf
https://www.ncsc.gov.uk/guidance/principles-for-ransomware-resistant-cloud-backups
https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available
https://www.ncsc.gov.uk/collection/10-steps
https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools
https://www.ncsc.gov.uk/information/cyber-security-training-schools
https://www.ncsc.gov.uk/collection/device-security-guidance
https://www.ncsc.gov.uk/information/early-warning-service
https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world
https://www.ncsc.gov.uk/collection/secure-system-administration

At CyberUK 2021 they did a specific session on ransomware which is well worth checking out.
https://youtu.be/FppzWedY0ic

Useful links

South East Cyber Resilience Centre

https://www.secrc.police.uk/
https://www.secrc.police.uk/helphacked
https://www.secrc.police.uk/_files/ugd/129c98_54825bebd62c4ecdb7816ebaa471258b.pdf

Action Fraud

https://www.actionfraud.police.uk/

CISA

https://www.cisa.gov/stopransomware
https://www.cisa.gov/stopransomware/ransomware-guide

SecureWorks

https://www.secureworks.com/research/ransomware-evolution

Cyber Griffin

https://cybergriffin.police.uk/

South East Cyber Crime Unit

https://southeastcyber.police.uk/
https://southeastcyber.police.uk/cyber-small-organisations/
https://southeastcyber.police.uk/cyber-large-organisations/

National Protective Security Authority

https://www.npsa.gov.uk/
https://www.npsa.gov.uk/security-campaigns