

Ransomware Awareness

for Hampshire Primary Schools



Hampshire County Council and Project Knapweed

8 May 2024

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

The evolution of ransomware
Threat to the education sector
Common myths

Quick break

2. Ransomware in the Wild

Real world experience
Project Knapweed
Impact to People

*Dark web demo
&
Break*

3. Prepare for Ransomware

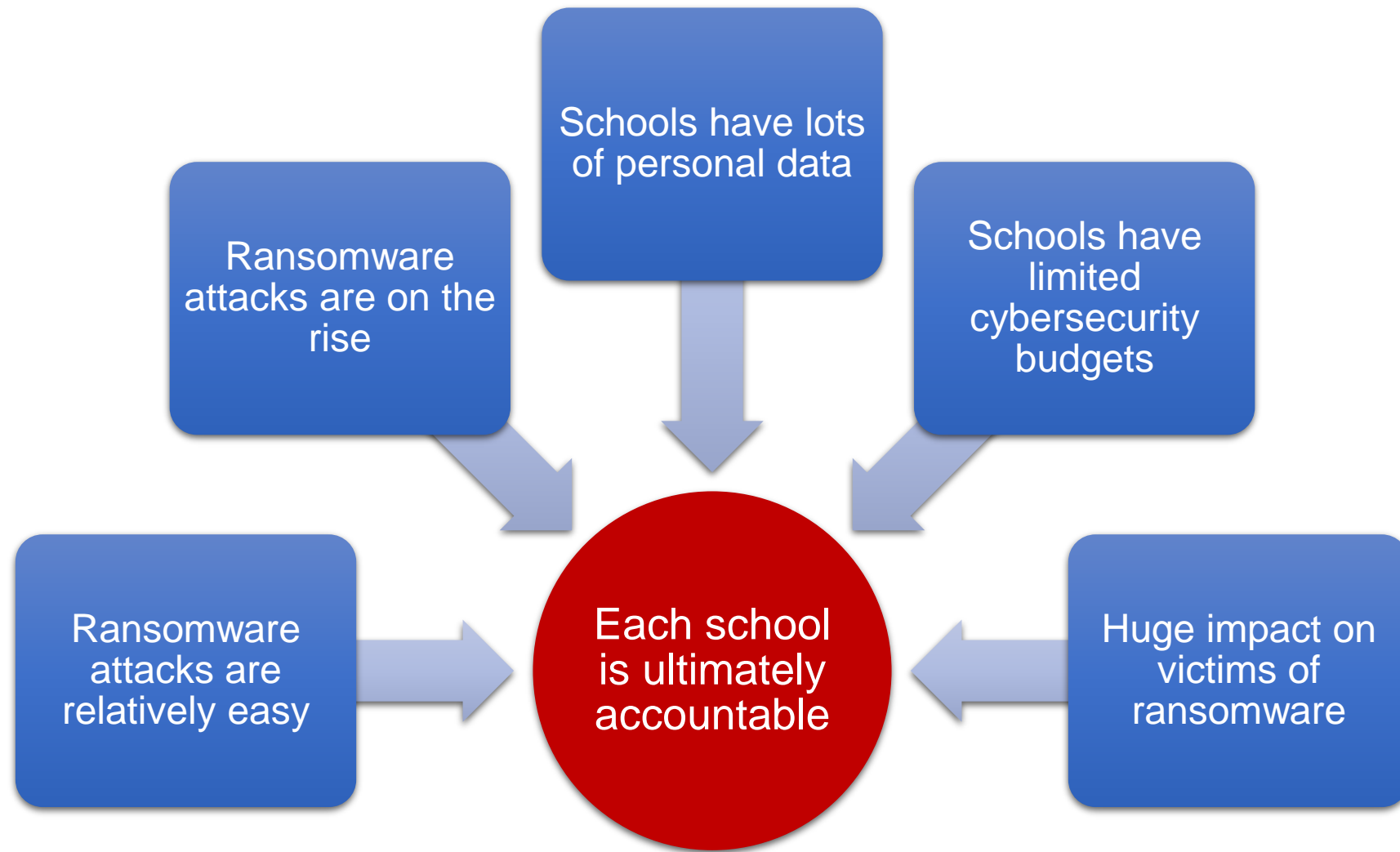
Proactive Steps
Technical Controls
What to do in worst case scenario

*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



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.

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.

2021

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

2016

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

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.

2022 to 2023

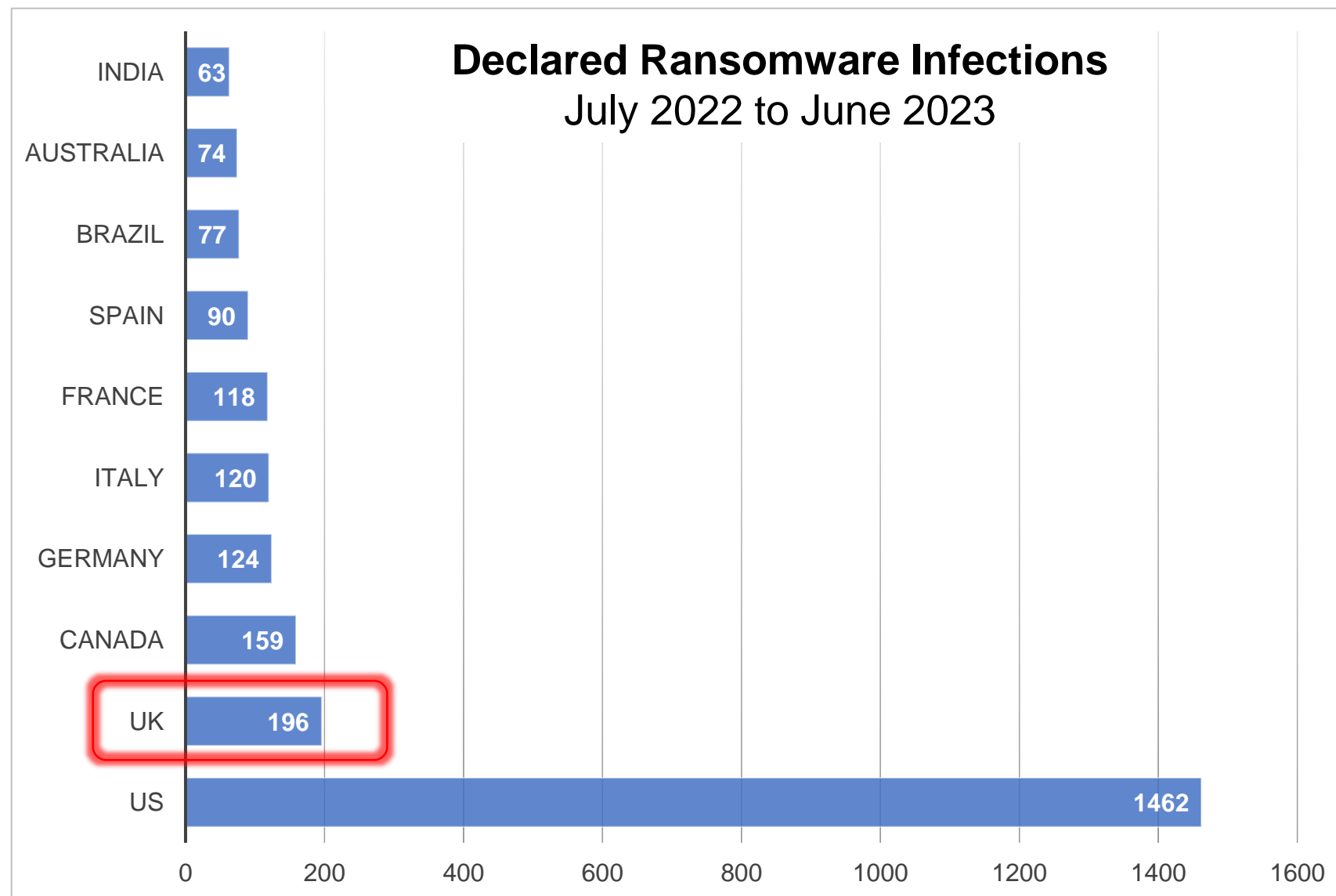
Successful ransomware attack on at least two Hampshire Secondary Schools.

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.



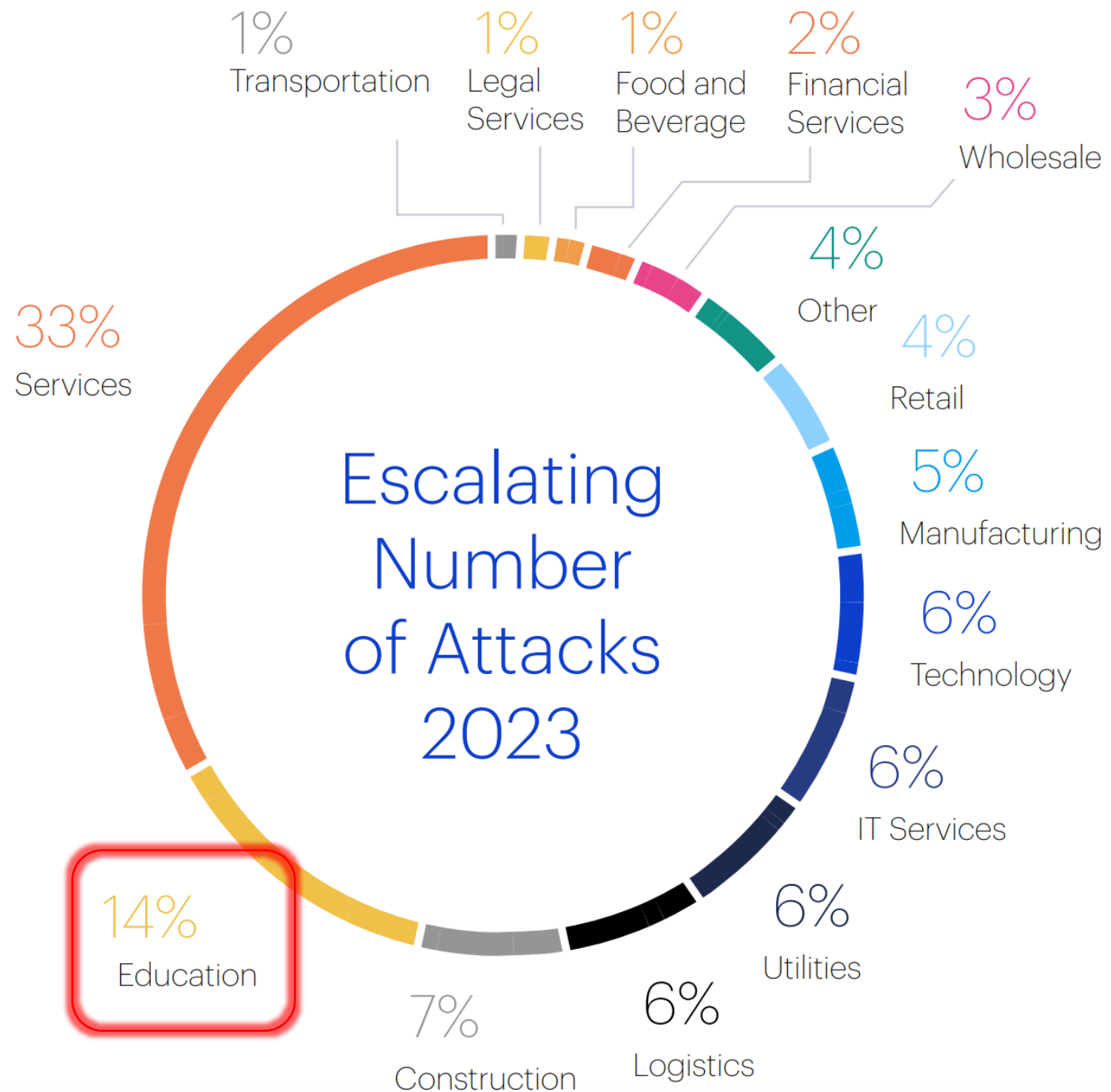
Source: Malwarebytes Ransomware Report for UK 2023.

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 2023

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



Source: Project Knapweed

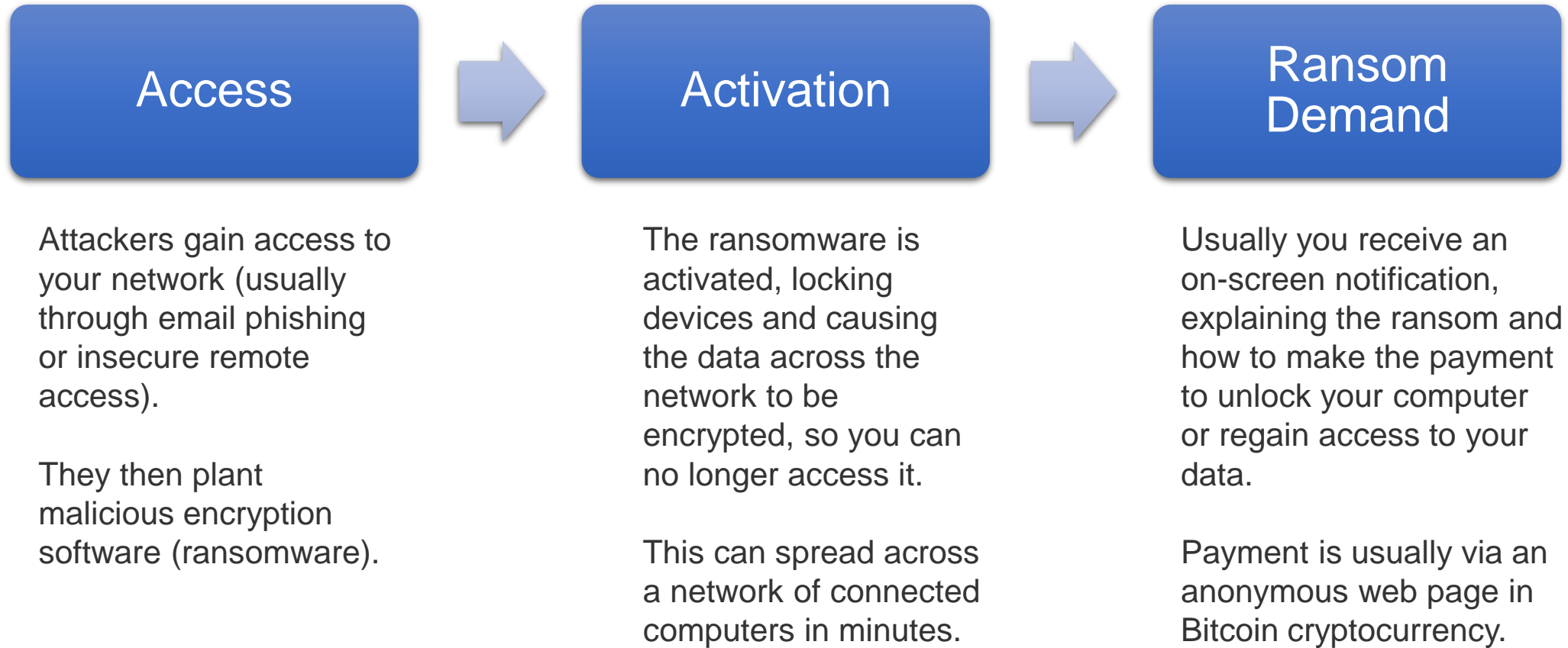
Ransomware in 2024

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

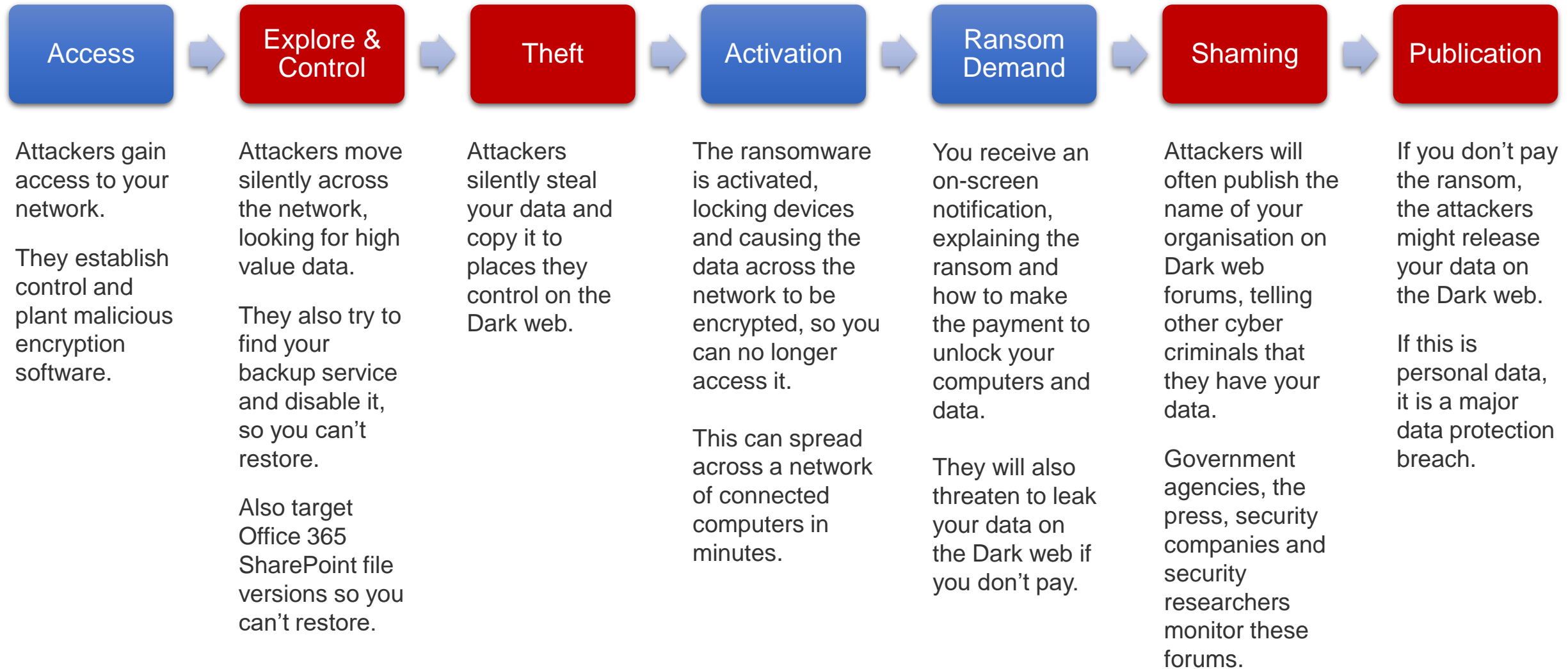


Source: Project Knapweed

How does it work?



How does it work now?





What is Phishing?

Sending fraudulent emails or messages that appear to come from a legitimate source, trying to:

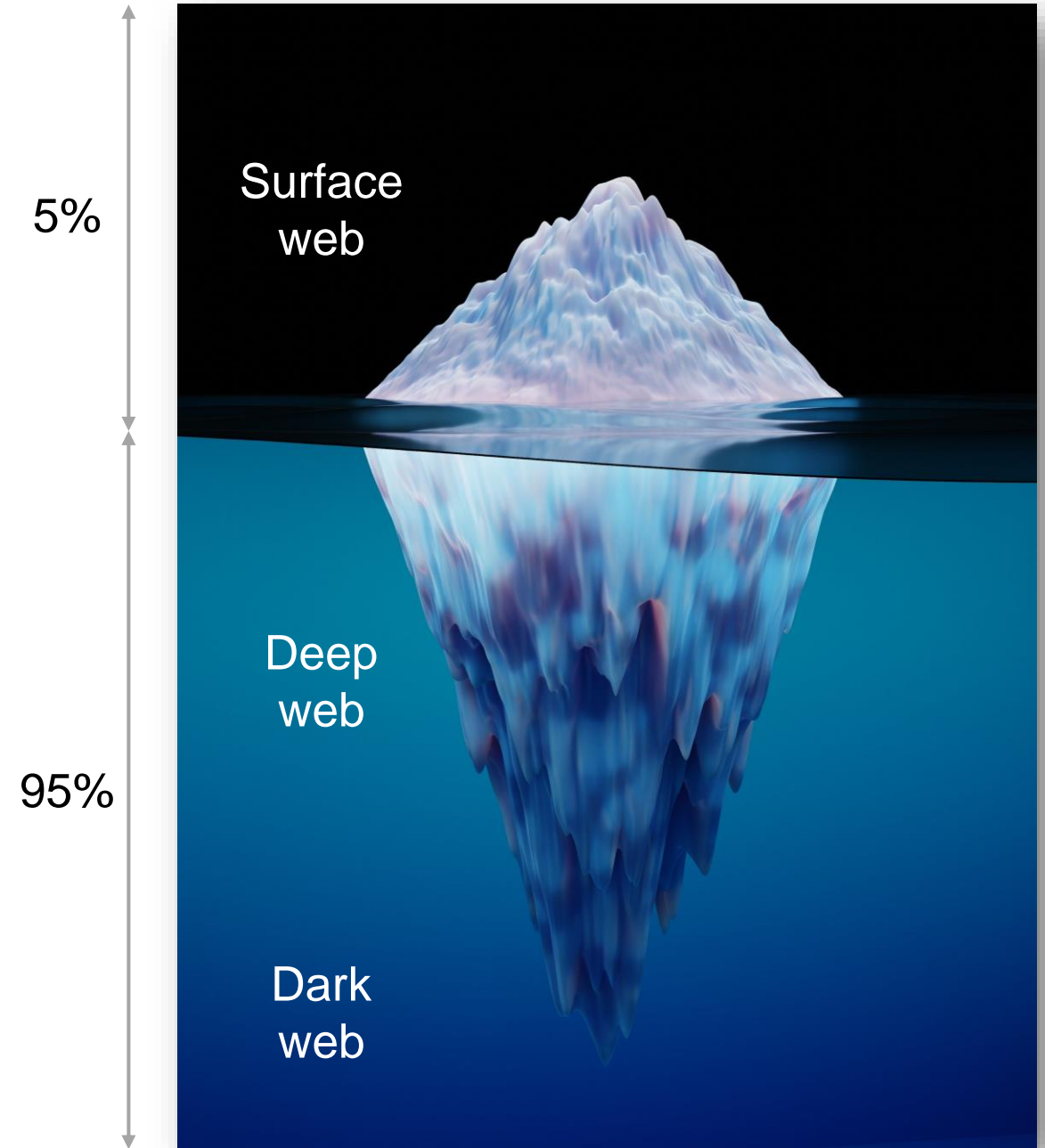
- **Steal Money:** Phishing attempts often trick victims into revealing sensitive financial information, such as credit card details or online banking credentials.
- **Gain Unauthorised Access:** By impersonating trusted entities, phishers aim to obtain login information for various accounts, including email, social media, and online services.
- **Install Malware:** Malicious links or attachments in phishing emails can infect victims' devices with malware (including ransomware).

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.**



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**.

Break



Part 2

Ransomware in the Wild



Bruce Thomson

Project Knapweed

ransomware

just theft, extortion and blackmail

May 2017 - Start of the ransomware as we know it now

The WannaCry attack wasn't specifically targeted at the NHS, but it did significantly impact them in May 2017. Here's a timeline of the event:

- Before May 2017: A vulnerability in Windows software is identified by Microsoft, and a security patch is released.
- Friday, May 12th, 2017: The WannaCry ransomware attack hits worldwide, targeting unpatched Windows PCs.
- May 12th, 2017: The NHS is impacted, with many hospitals and GP surgeries experiencing disruptions.
- Within 24 hours: The spread of the attack is contained due to a fortuitous discovery of a "kill switch".

Following days and weeks: The NHS works to recover from the attack, with some cancellations of appointments and procedures.

Government puts cost of WannaCry to NHS at £92m



The Department of Health and Social Care (DHSC) has estimated that WannaCry cost the NHS £92m in direct costs and lost output.

2017-2021

From a slow start, and moving away from network virus attacks there was a gradually growing number of ransomware attacks, first came data encryption as the primary attack method, then by mid 2021 dual attacks with some exfiltration of data, leading to data exfiltration being part of every attack by mid late 2021

During **COVID**, all the ransomware operators moved to **The Onion Routed Network**, (*aKa TOR or the darkweb*), this offers much in terms of anonymity which is the design purpose of the dark web.



Spring 2022

In discussion with Alan Hunt @ Hytec we concluded that SOC (Security Operations Centres) and those running SIEM (System Information Event Management) systems had poor intelligence on ransomware and dark web activities.

Hytec kindly met the compute/web-server costs and shared with wider UK public sector organisations.

So I made this, and something happened!



Project Knapweed: Dark-web ransomware group tracking APP 07:19

3 new ransomware attacks detected in the last 24hrs [\[click this link for more details\]](#)

This service currently scans 130 dark-web based ransomware groups to provide data on when they announce their attacks, note that this is often at the end of a long process/cyber attack. This list is updated daily, it also includes some downloadable data that has .onions and clear/surface web domains for ransomware sites as well as related data digests. Please use this data carefully and heed the guidance at the bottom of the web page, and finally please note that whilst sanitation efforts... (edited)

api.red-team.cloud

Sponsored by Hytec Managed 24/7 Security Services

Managed Security and Governance, Risk, and Compliance specialists for Local Government and Health.

Why a Sponsor?

This is service free to the UK public sector, sponsors can come and go and it helps if you click and visit their website!

Costs are covered until April 2025, (note the link below expires after fourteen days)

<https://api-v2.red-team.cloud/rss/20240507070003.html>

Activity detected over the last 24hrs

Since the last check we can count 18 new attacks reported by the dark-web ransomware gangs that we are tracking, these are as follows:

Date-Time - Group - Data Snippet Offered
2022-10-30 16:58:07 - lockbit3 - byp-global.com
2022-10-30 16:58:04 - lockbit3 - cacula.com
2022-10-30 16:58:19 - lockbit3 - close-upinternational.com.uy
2022-10-30 16:58:12 - lockbit3 - gruposanford.com
2022-10-30 16:58:10 - lockbit3 - hoosierco.com
2022-10-30 16:58:10 - lockbit3 - macrotel.com.ar
2022-10-30 16:58:16 - lockbit3 - seamlessglobalsolutions.com
2022-10-30 16:58:10 - lockbit3 - sociedadbilbaina.com
2022-10-30 16:58:17 - lockbit3 - zurifurniture.com
2022-10-30 18:44:45 - lockbit3 - aaanchorbolt.com
2022-10-30 18:44:48 - lockbit3 - bellettiasensori.it
2022-10-30 18:44:44 - lockbit3 - coopavegra.fi.cr
2022-10-30 18:44:48 - lockbit3 - exco.fr
2022-10-30 18:44:46 - lockbit3 - happmobi.com.br
2022-10-30 18:44:43 - lockbit3 - santimuni.com
2022-10-30 18:44:49 - lockbit3 - will-b.jp
2022-10-30 20:56:26 - snatch - HENSOLDT France
2022-10-31 06:52:55 - lockbit3 - thalesgroup.com

This work is currently sponsored by



The Hytec Managed Security Platform. Designed by necessity, our service addresses the very particular set of issues faced by local authorities and other public sector and 3rd sector organisations.

Working in security and information governance for over two decades Hytec has established a comprehensive, best in breed Managed Security Service that will significantly enhance the protection of systems/data, help achieve your compliance requirements and ensure appropriate security mechanisms are in place.

Digests and Resources:

A complete List of ransomware attacks (date, group and snippet of data in a .csv format):

[Click here to download](#)

Digest of the most recent 100 ransomware attacks (date, group and snippet of data in a .csv format):

[Click here to download](#)

Intelligence gathered on ransomware gangs (.csv format):

[Click here to download](#)

Surface web sites linked with or holding ransomware data:

[Click here to download](#)

Links to .onion web sites linked with ransomware data:

[Click here to download](#)

(The links within these last two files maybe ephemeral or offline from time to time)

Late autumn 2022

November 2022 at a meeting of the Cyber Technical Advisory Group (CTAG.gov.uk), I first raised my observation of what I called “Associated Data”

Associated data - data that is exposed in the clear (on the dark web, and occasionally on the surface web) as a result of a ransomware attack on an organisation that is the property of someone else (supply chain data may better describe this)

Spring 2023 Project Knapweed

- **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 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 or two...***

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

Spring 2023

Cambian - centred many people's thinking about this in the wider UK public sector with many councils impacted

Keen Group - a south east London Taxi firm also demonstrated more localised but harmful impacts of data exfiltration and subsequent open access to it

The complexity of the levels of support for this type of attack, and the impacts, become clearer, those attacked are often poor at notification of those whos data maybe exposed.

Cambian = Associated supply chain Data (Jan 2023)

Data stolen (exfiltrated), and available to view and download on the AvosLocker website, includes 263700+ files mainly MS Office Word, Excel and PDF, including staff payroll, and client (child) data.

Total volume 135GB (note the .txt file list was 43MB)

- 12GB ./bythebridge.co.uk
- 44GB ./cambianguroup.com
- 80GB ./caretech.co.uk

Also noted, a number of files with “passwords” in their name and several .PST files.

Knapweed: An early safeguarding success



CareTech UK

By email

Date

Dear Sirs

On behalf of the Local Authorities shown below, we are contacting yourselves to escalate our ongoing concerns regarding Cambian's leadership response to the 4th January 2023 Cyber Incident to a complaint. In particular:

Keen Group = Another Associated Data event Feb 2023

An attack by **ALPHV** (aKa Black Cat) on The Keen Group took place in February 2023. As a result, exfiltrated data was published on 23rd February 2023, and includes information relating to several London Boroughs. The Keen Group are a minicab firm who offer services mainly in and around the South East of London but specialise in the transport of children and adults with special needs.

We are making you aware of this breach as a WARP member and would suggest that you raise this internally with social care so that they may contact the Keen Group directly for further information. We can provide a file list of the exposed data on request which may help you in your investigations.

Matt Smith	Data breach - The Keen Group - Hi Stephen, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen ...
Matt Smith	Data breach - The Keen Group - Hi Owen, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen Gro...
Matt Smith	Data breach - The Keen Group - Hi Mary, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen Gro...
Matt Smith	Data breach - The Keen Group - Hi Mal, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen Group...
Matt, Ben 2	Data breach - The Keen Group - Hi Ben, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen Grou...
Matt Smith	Data breach - The Keen Group - Hi Matthew, Through Project Knapweed, we have been made aware of an attack by ALPHV on The Keen ...



The dark web

what is it? ..and why do we have it?

The Dark Web - yes, dark because/..

While its part of the internet it

- It works in a slightly different way
 - TCP/IP yes
 - DNS no
 - Makes search engines, more like commercial phone directories (yellow pages) the site owner has to register
 - Its focus is being anonymous for site owners and visitors
- Needs a special browser - the Tor Browser
- Strongly recommended is a VPN - Use one that does not keep logs, Nord is okay for this, there are many others, *also useful for when travelling too!*

The Dark Web - Why do ransomware groups use it?

Anonymity is key here

- They attack they leave a note to an “onion” address and its hard, if not impossible to find, only they and you (at that point their victim know).
- However they like are human love to brag, so researches like the Knapweed team and many other good folks can track them

[Donate Now](#)[About](#) [Support](#) [Community](#) [Blog](#) [Donate](#)[English \(en\)](#) ▼[Download Tor Browser](#) ▼

Download Tor Browser

Protect yourself against tracking, surveillance, and censorship.

[Download for Windows](#)[Signature](#) ⓘ[Download for macOS](#)[Signature](#) ⓘ[Download for Linux](#)[Signature](#) ⓘ[Download for Android](#)[Download for another platform](#)[Download the latest alpha build](#)[Download Tor](#)

ahmia.fi - juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

AHMIA

Ahmia searches hidden services on the Tor network. To access these hidden services, you need the [Tor browser bundle](#). Abuse material is not allowed on Ahmia. See our [service blacklist](#) and report abuse material if you find it in the index. It will be removed as soon as possible.

For more about Ahmia, see [indexing information](#) , [contribute to the source code](#).

[The Tor Project](#)

Onion service: juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

<https://tor.taxi/> -

This site is helpful:

- At the top is a list of sites to avoid!
- Also a history of the dark web, which is worth a read

These links only work on Tor, but this web site can be seen on the surface.

The BBC, CIA and Pornhub ?

<http://tortaxi7axhn2fv4j475a6blv7vwjtpieokolfnojwvkhshnj7sgctkqd.onion/>

tor.taxi - your ride to the darknet

Click here to visit our onion address!

Click here to view links you should avoid!

Go to /sitename to view more mirrors and signed links! E.g: /dread

Interested in the history of the darknet? Click here to read our darknet journal!

PSA: Cannazon Market has retired!

News

Darknetlive

DarknetHub

Darknet Inside

The New York Times

BBC

ProPublica

Dutch National Police

CIA's Official Onion Site

USA's NCIDE Task Force

Markets

ToRReZ

World

Dark0de

Versus

Monopoly

ASAP

Cannahome

Cannazon

Cartel

Incognito

Search Engines

Archetyp

Forums

Dread

The Hub

CryptBB

The Majestic Garden

Envoy

NZ Darknet Market Forum

Torigon

SuprBay

Raddle

Verified

Deutschland im Deep Web



Ransomware attacks

Are just one kind of cyber attack

Ransomware attacks are:

NOT sophisticated

Do the easy stuff:

Get ready: Schools and community organisations could do worse than use this [template](#) and set a cyber response plan (maybe set a small group of IT savvy parents or governors loose on it to do the groundwork or thinking).

Enture there is two form factor on everything, yes its pfaff, but, both these the result of not doing this:

- Small UK district council - Office 365 and £4m - *no mfa*
- Large US healthcare provider - Office 365 \$.8 billion (so far) - *no mfa*
- School 1 - Kent, a parent IT Support - Network access to everything
- School 2 - Cornwall was a pilot for a new ransomware group - unlucky?

...so how are targets selected, is there a link?



Ransomware attacks are:

NOT sophisticated

Do your best, learn how to find and patch vulnerabilities on your systems, do not blame your ICT support staff - defend as one!

L3 Harris could not defend...

L3 Harris?



DELIVERING THE SHARED COMMON OPERATIONAL PICTURE

The modern battlespace is more data rich than ever. L3Harris C5ISR systems expertise ensures commanders have access to the complete battlefield picture they need.



RESILIENT NETWORKS



ISR SENSORS

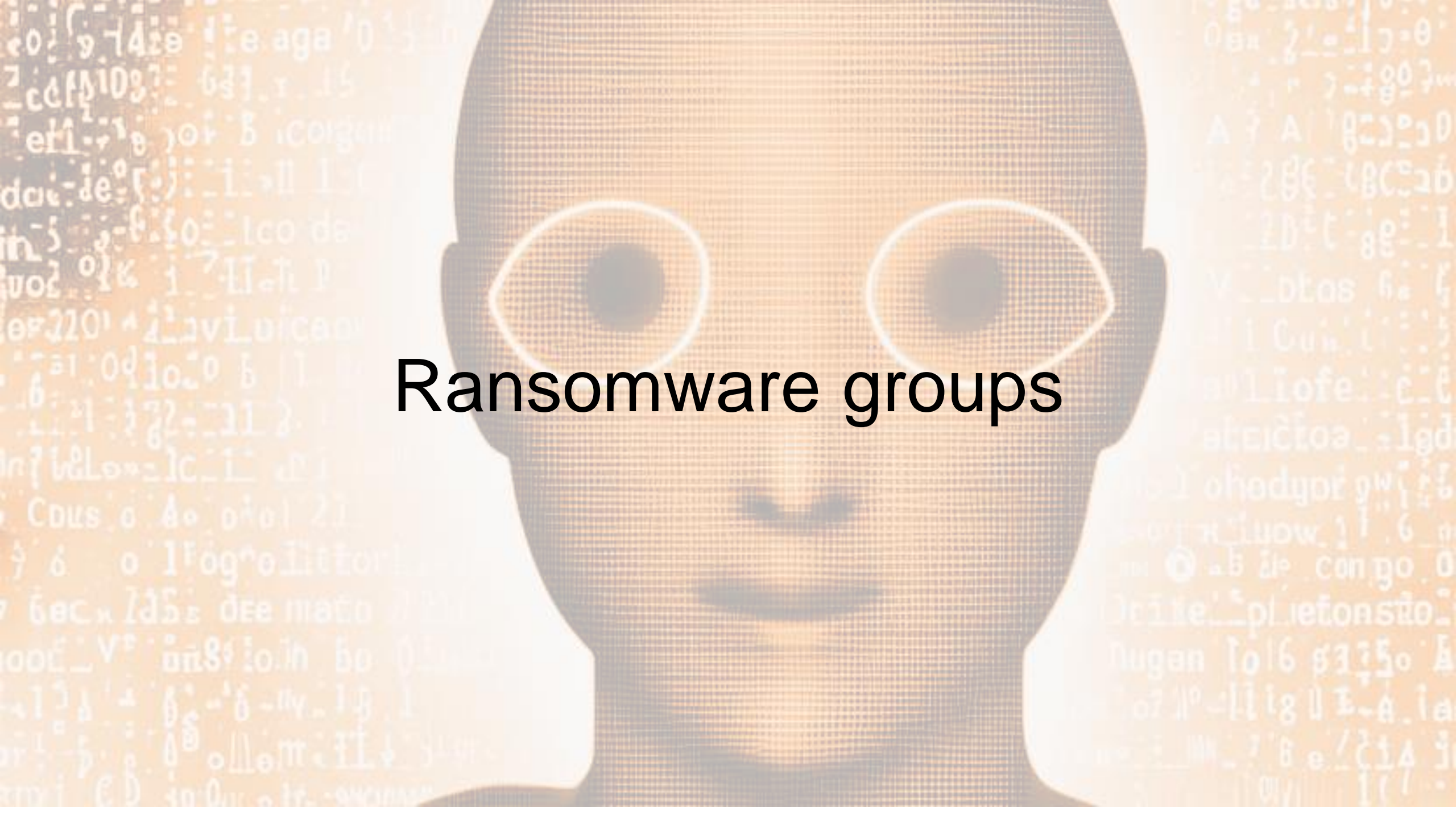


AI/MACHINE LEARNING



DATA CENTRICITY

Ransomware groups

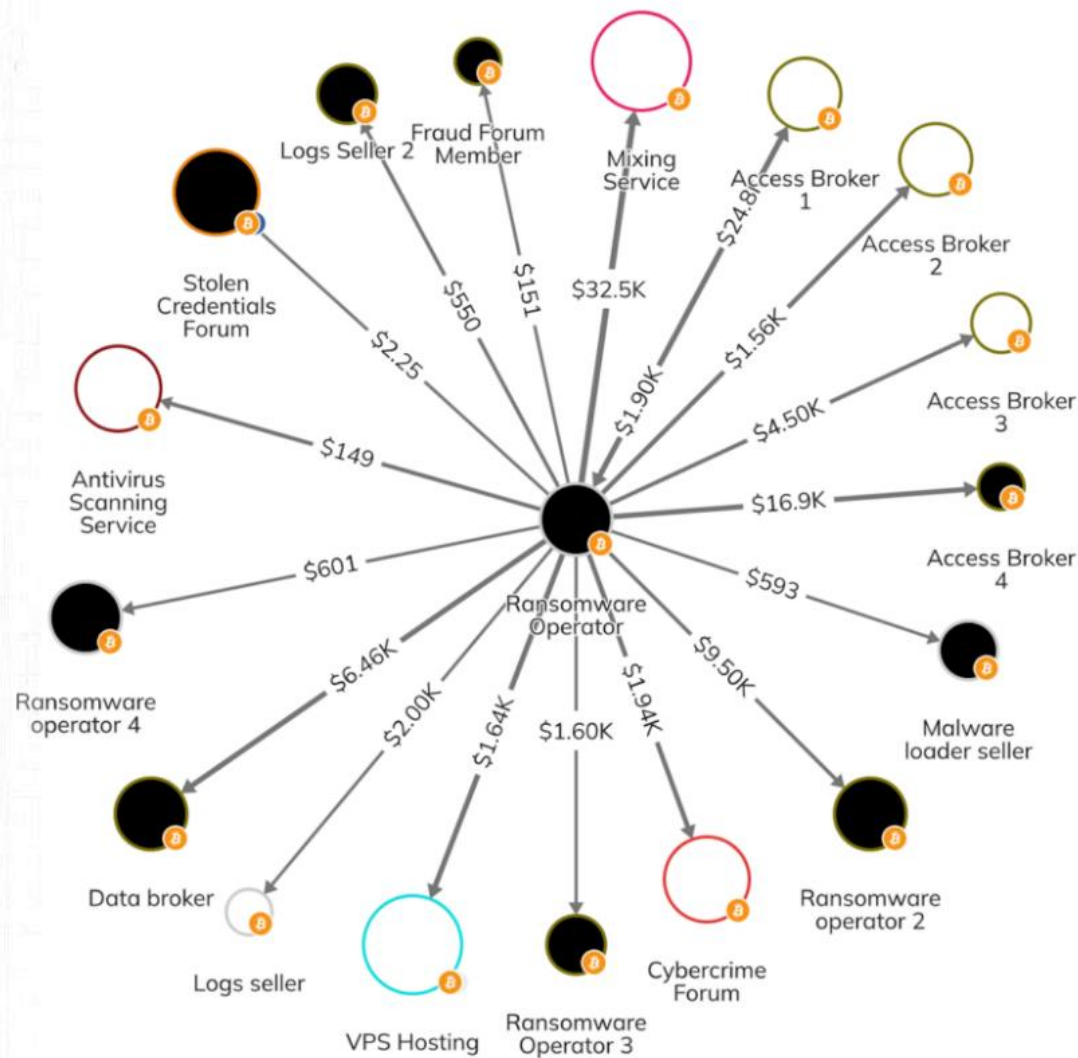


Ransomware Groups - Have a supply Chain

The spread of Ransomware-as-a-Service (RaaS) and growth of IABs

- The growth of initial access brokers (IABs) as their name would suggest, IABs penetrate the networks of potential victims, then sell that access to ransomware attackers for as little as a few hundred dollars.
- Analysis of cryptocurrency transaction often finds a correlation between inflows to IAB wallets and an upsurge in ransomware payments, suggesting monitoring IABs could provide early warning signs and allow for potential intervention and mitigation of attacks.
- IABs combined with off-the-shelf RaaS, means that much less technical skill is required to carry out a successful ransomware attack.
- We can see examples of this activity on the Reactor graph that follows, which shows a ransomware operator sending funds to several IABs and other purveyors of tools useful for ransomware attacks.

Ransomware Groups - Supply Chain



Ransomware Groups - Say nothing Pike?

Outside of the Public Sector reporting of breaches to external authorities and organisations is also low.

The report from the Department for Science, Innovation and Technology (DSIT), released today, painted security as more of an afterthought for UK businesses, especially when considering the figures about how breaches are handled.

- Only 10 percent of businesses ring the police when they detect the most disruptive breach in the previous 12 months – *a stat that's halved when looking at who reports incidents to the National Cyber Security Centre (NCSC)*.
- Reporting rates to arguably the most important entity, the Information Commissioner's Office (ICO), weren't even included in the report since the watchdog didn't make the top ten organizations that receive reports of breaches.
- Banks, building societies, and credit card issuers, on the other hand, placed first – 32 percent of businesses reported incidents to them.

Clients and customers were only alerted 5 percent of the time.

https://www.theregister.com/2024/04/09/uk_biz_response_to_cybercrime/ - easy to read version!

A stylized, pixelated face in shades of brown and tan, centered in the background. The face has large, dark eyes and a simple, straight line for a mouth. The background is a light beige color with faint, repeating binary code (0s and 1s) scattered across it.

the spring 2024

tactical briefing

Spring 2024

Tactical update: New developments in extortion and pressure - Leicester City Council

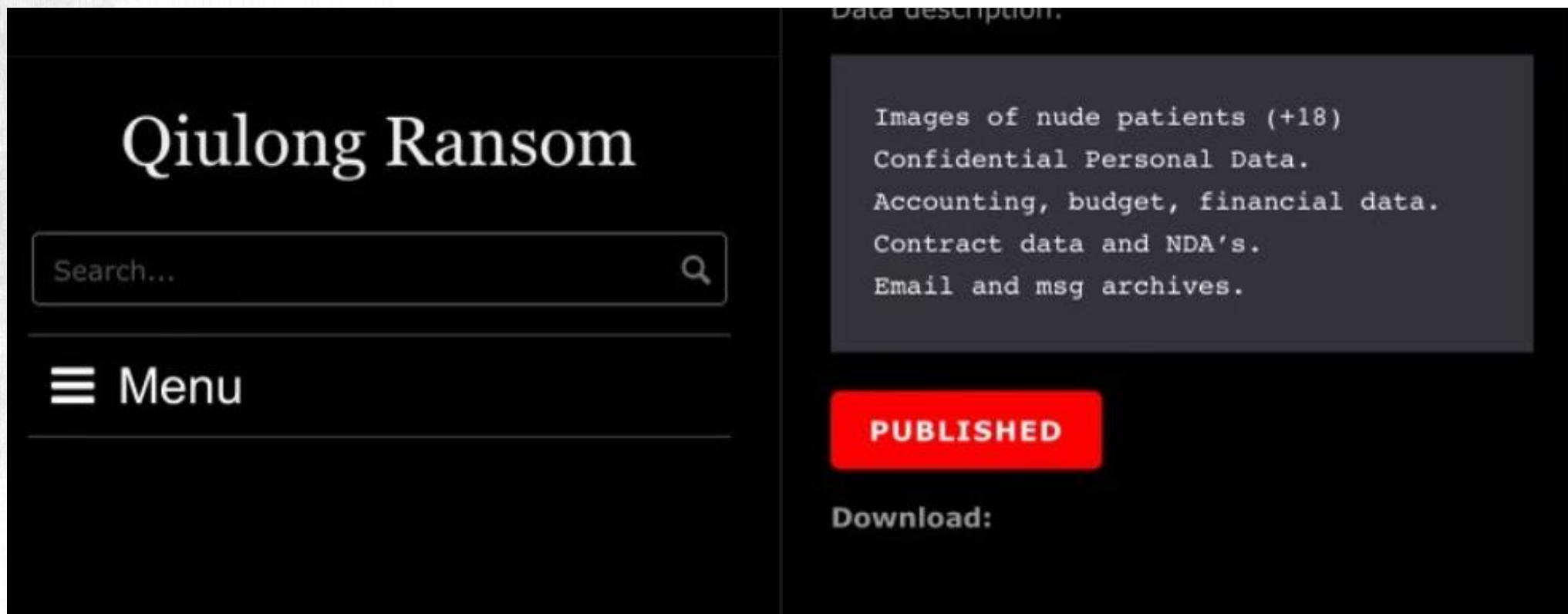
- The quick show and tell (proof pack)
- The vertical proof pack

Elsewhere: - evolving pressure tactics and making use of best practice!

- Threat to report victim by the RW group to regulatory authorities for under declaration
- Use of the stolen data, to put direct stress on to the customers of the victim (in the form of a SWAT team)
- Use of data that would embarrass or cause reputational harm to the victim such as illegal or or lurid searches for things like extreme pornography (CP)
- Encrypting file names and not files, or part encryption of files

Spring 2024

New Qiulong Ransom: Maybe the worst first post I can remember leaking nude plastic surgery patient photos as the proof pack.



Who is attacking schools? – 6th Jan BBC 2023

- 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



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

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.

Institute of Science and Technology Austria

<http://www.ista.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!!!


Can things get any worse?

19. 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
ISA 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	21:43
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 Obseations - Confidential.docx	06-Jan-2023	22:25
09092016 All Obseations - Confidential.docx	06-Jan-2023	22:35
09092016 Duty Manager Rota.doc	06-Jan-2023	21:49
09092016 KTH Obseations - Confidential.docx	06-Jan-2023	21:50
09092016 NWI Obseations - Confidential.docx	06-Jan-2023	21:25
09092016 Obseations - Confidential.docx	06-Jan-2023	21:25
09092016 PCA Obseations - Confidential.docx	06-Jan-2023	21:32
09092016 PHA Obseations - 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&SocialCareCP Resources/	16-Feb-2015	01:21

Spring 2024 - 19th/20th Feb




LEAKED DATA



Press Releases


PUBLISHED



Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks


PUBLISHED



Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp


PUBLISHED



Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?


2D 18H 38M 26S



Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys

PUBLISHED



Law Enforcement may be able to assist you to decrypt your Lockbit encrypted

Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool


PUBLISHED

Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family

Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments

PUBLISHED



FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.

Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions

0D 3H 8M 26S

United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity

Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland

PUBLISHED

On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French

Activity in Ukraine

PUBLISHED

On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.


Report Cyber Attacks!


PUBLISHED

Please report your Cyber Incident. To enable Law Enforcement to take protective and


Cyber Choices


PUBLISHED







LEAKED DATA





THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE





US Sanctions

The cyber-related sanctions program implemented by the Office of Foreign Assets Control (OFAC) imposes sanctions on threat actors responsible for malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States. The following malicious cyber actors have been sanctioned for their involvement in LockBit Ransomware.


- Ivan Kondratyev (Bassterlord)
- Artur Sungatov


Links:


- <https://home.treasury.gov/news/press-releases/jy2114>


UPLOADED: 20 JAN, 2024 13:21 UTC


UPDATED: 07 FEB, 2024 10:06 UTC












































Spring 2024 - 26th Feb


Spotted by a Knapweed team member LB3 back in business! - With new, possibly AI based tools!!

The CIR suggested that data had not been exfiltrated, however, it showed up on the Lockbit3 site, around 2.5 to 3gb but not in the original folders as we have come to expect.

- This had been sorted into folders “bank - lots of bank details culled form various documents in finance and payroll and staff folders” “passports - it was a school so these had all be gathered up from various directories ” “cyber - looking for cyber insurance perhaps, and the value”?
- This suggests a reduction in the amount of data stolen, but a more focused approach, perhaps automated search patterns for specific higher value data,




Spring 2024 - 5th May

<demo>




LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE
UK, THE US AND THE CRONOS TASK FORCE

Press Releases


1D 17H 46M 5S



Updated: 02 May, 2024, 13:37 BST 30

Who is LockbitSupp?


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 30

But there's more...


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 20

What have we learnt?


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 14

More LB hackers exposed


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 14

What have we been doing?


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 15

Preventing and protecting


1D 17H 46M 6S



Updated: 02 May, 2024, 13:37 BST 11

Report Cyber Attacks!

1D 17H 46M 6S




Updated: 02 May, 2024, 13:37 BST 6



Close



4D 17H 46M 6S



This leak site (lockbit blog) to close.



LEAKED DATA

 TWITTER
 PRESS ABOUT US

 HOW TO BUY BITCOIN
 AFFILIATE RULES

 CONTACT US
 MIRRORS

peaseinc.com

3D 00h 36m 28s

Based out of Lakewood, Washington, Pease Construction has been delivering construction services to public and private clients for over 35 years. Our success relies on having a team of

Updated: 01 May, 2024, 07:53 UTC 3917

yupousa.com

3D 00h 38m 16s

YUPO is the recyclable, waterproof, tree-free Synthetic Paper with attributes and properties that make it the perfect solution for a variety of marketing, design, packaging and labeling

Updated: 01 May, 2024, 07:53 UTC 3836

concorr.com

3D 00h 32m 15s

CONCORR, Inc. was established in 1990 to develop technologies and provide solutions for mitigating corrosion of reinforcement, both conventional and stressed, in reinforced

Updated: 01 May, 2024, 07:50 UTC 3840

cordish.com

3D 00h 33m 45s

The Cordish Companies' origins date back to 1910 and encompass four generations of privately-held, family ownership. During the past ten decades, The Cordish Companies has

Updated: 01 May, 2024, 07:48 UTC 3807

colonial.edu

3D 00h 30m 26s

The Colonial School District draws approximately 5,400 students from the Borough of Conshohocken, and the Townships of Plymouth and Whitemarsh in Montcoermey

Updated: 01 May, 2024, 07:45 UTC 3783

bluegrasstechnologies.net

3D 00h 28m 32s

BLUEGRASS TECHNOLOGIES INC. Environmental Consulting and Abatement Contractor for Asbestos, Mold and Lead

Updated: 01 May, 2024, 07:43 UTC 3611

anatomage.com

3D 00h 26m 10s

Anatome enables an ecosystem of the next-generation 3D anatomy software and hardware, delivering innovations for multidisciplinary applications.

Updated: 01 May, 2024, 07:42 UTC 3605

alimmigration.com

3D 00h 23m 13s

Registered Migration services with office located in Florida.

Updated: 01 May, 2024, 07:38 UTC 3617

hookerfurniture.com

3D 00h 18m 38s

A billion revenue furniture corporation with over dozen brands BUT do not care for the data of their customers and own company. Founded by

Updated: 01 May, 2024, 07:38 UTC 3617

sierraconstruction.ca

5D 11h 02m 37s

Sierra Construction is a general contracting firm located in Kenora, Ontario. We specialize in commercial, residential and industrial

Updated: 01 May, 2024, 07:38 UTC 3617

sbsobak.com

1D 18h 55m 23s

About SBS of Bakersfield, Inc. SBS of Bakersfield specializes in document-based technology solutions. SBS of Bakersfield helps

Updated: 01 May, 2024, 07:38 UTC 3617

ottlite.com

PUBLISHED

OttLite was founded in 1989 by Dr. John Nash Ott to bring the power of natural daylight indoors through his one-of-a-kind natural daylight bulb

Updated: 01 May, 2024, 07:38 UTC 3617

Dmitry Yuryevich Khoroshev ?

<https://nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned>

Spring 2024 - 7th May

<demo>

SPECIALLY DESIGNATED NATIONALS LIST UPDATE

The following individual has been added to OFAC's SDN List:

KHOROSHEV, Dmitry Yuryevich (a.k.a. KHOROSHEV, Dmitrii Yuryevich; a.k.a. KHOROSHEV, Dmitriy Yurevich; a.k.a. YURIEVICH, Dmitry; a.k.a. "LOCKBITSUPP"), Russia; DOB 17 Apr 1993; POB Russian Federation; nationality Russia; citizen Russia; Email Address khoroshev1@icloud.com; alt. Email Address sitedev5@yandex.ru; Gender Male; Digital Currency Address - XBT bc1qvhnfknw852ephxyc5hm4q520zmvf9maphetc9z; Secondary sanctions risk: Ukraine-/Russia-Related Sanctions Regulations, 31 CFR 589.201; Passport 2018278055 (Russia); alt. Passport 2006801524 (Russia); Tax ID No. 366110340670 (Russia) (individual) [CYBER2].

Some of LockbitSupp a/k/a Dmitry Khoroshev's data and PII was exposed as a result of a Yandex data breach.

It exposes his address and food order history. It shows him ordering Cheesecake Factory semi-frequently.

Information via [@Info_IntelX](https://twitter.com/Info_IntelX)

Dmitry Yuryevich Khoroshev ?

<https://nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned>

Spring 2024 - IAB & Relentless scanning

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 companies 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).

Spring 2024 - often overlooked

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

For example, we have witnessed 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.

Spring 2024 - IOC / Detection and Hunting

(Old, but still valid)

- 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 given or 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 to 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?

Qs

more on dark web, ransomware and email!

<https://ctag.gov.uk>



Attribution & Thanks

“Leg-up” research

Josh NZ for some backend code

**App & web servers
Services)**

@HytecCyber (Hytec Manager Security

R&D Environment

@1uglycrazyroboT

QC

@waoaoms

AI Art

nightcafe.studio

**Project Knapweed
*contributors***

A small group of committed sometimes

Contact via

@cryptomoose@infosec.exchange

Or brucet@ctag.gov.uk / bruce.thomson@isfl.org.uk



This work is licensed under a
Creative Commons Attribution
4.0 International License.

Dark Web Demo and Break



Part 3A

Prepare for Ransomware



Rob Tillman
Hampshire County Council

Proactive Recommendations

Prepare


- Baseline your school
- Create a response plan and business continuity plan
- Promote staff engagement and training


Prevent

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

Prepare - 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>

Cyber Aware 

 National Cyber Security Centre

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

☐ Yes

☐ No / not sure

[Continue](#)

Prepare – Response Plan

Key aspects

- Agree pre-approved actions.
- Make decisions.
- Know who you need to talk to.
- Have pre-canned statements for parents and the press.
- Know how to isolate your network.
- Know how to turn off access to systems.
- Know how to secure your offline backups.



Department
for Education

Risk Protection Arrangement (RPA) Cyber Response Plan

- <https://www.rpaclaimforms.co.uk/wp-content/uploads/2022/03/RPA-Cyber-Response-Plan-Template-V1.0.pdf>

Prepare – Business Continuity Plan

Key aspects (business continuity IT related)

- Know what data you have.
- What are your business-critical systems.
- Know what do you need available to run the school.
- Know who your stakeholders are.
- Know what your endpoints are.
- Know what is on your network.
- Know who you connect to and what data they hold on your behalf.
- Document how to recover your IT



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.
- Get staff thinking about their digital footprint
- Cultivate a culture of shared responsibility.
- Promote open discussions.



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).
- Don't use USB sticks for data transfer.
- Don't allow staff administrative rights over their devices.



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



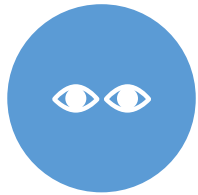
Trust but Verify

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



Adversary Tactics



Deception

Emotional
Stress

Time
Pressure

Isolation

Greed

Exploitation

Prevent – Cyber Security Frameworks

Backup your data	Protect from Malware	Keep all your devices safe	Password protect data	Avoid phishing emails
<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Install Anti Virus and ensure it is maintained• Stop staff downloading unauthorised software.• Ensure software patches are applied and keep software up to date.• Control USB• Enable firewalls	<ul style="list-style-type: none">• Password protect all devices.• Make sure you can remote wipe devices.• Ensure software patches are applied and keep software up to date.• Don't connect to unknown networks	<ul style="list-style-type: none">• Turn on passwords wherever possible.• Use Multi Factor Authentication.• Avoid predictable passwords• Change all default passwords.• Password managers.• Don't reuse passwords	<ul style="list-style-type: none">• Restrict accounts• Report all attacks• Check your digital footprint• Stop, Think, Breath (user training)

Prevent - 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

Prevent - Prevent delivery – User Aspects

The simple things

- All accounts should have strong passwords.
- Two factor authentication should be enforced on all accounts.
 - Including School social media accounts.
- Avoid password reuse.
 - (work and personal shouldn't meet!)



Prevent - Prevent delivery - IT Team

Secure By Design

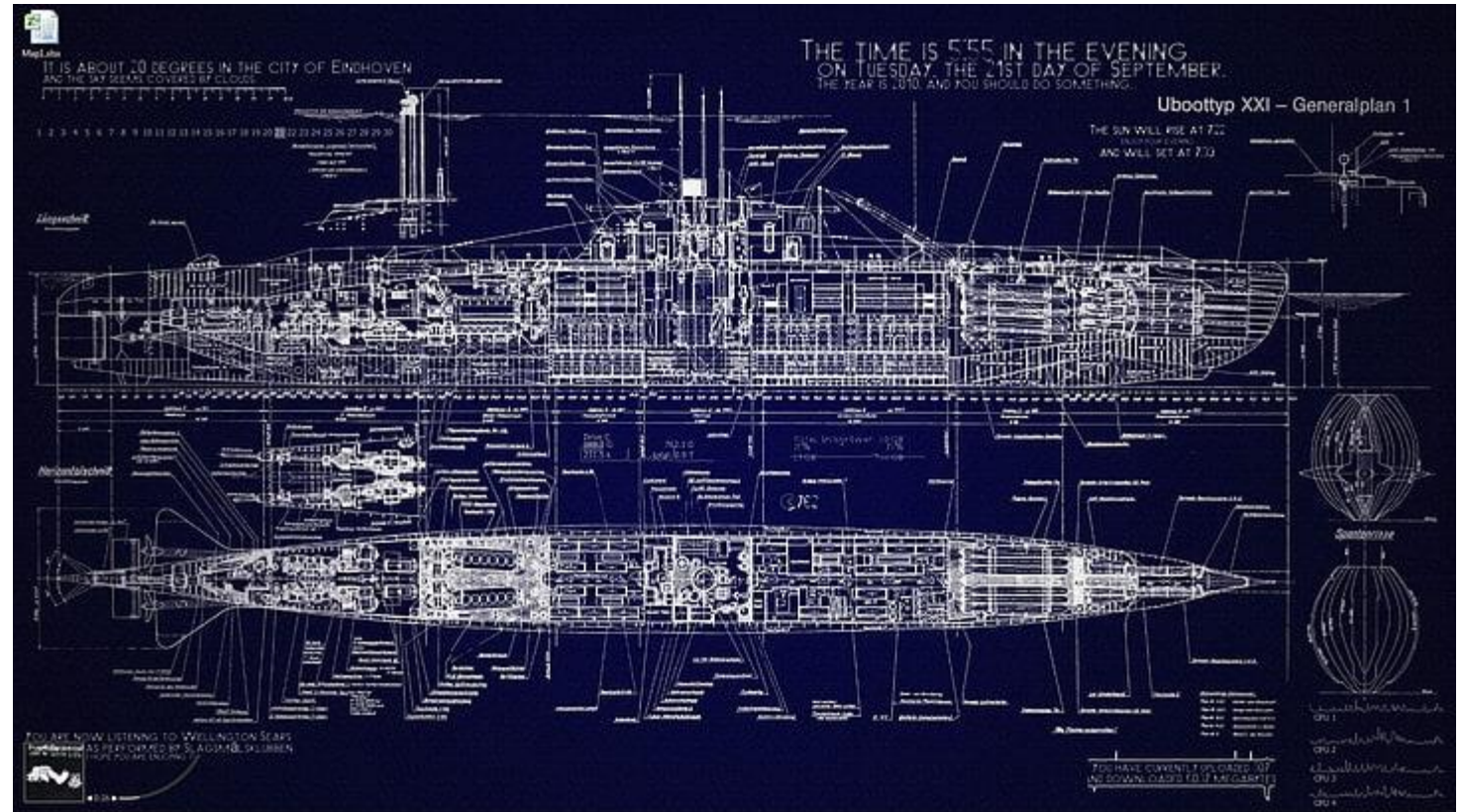
Network segmentation

Software good practice

Control externally facing systems

Multi factor authentication

Least privilege



Prevent - Prevent It Spreading

Device 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.

Prevent - Monitor and Alert

Ensure alerts are generated from -

- Anti Virus software
- Azure Tenancy warnings

Look at adopting -

- NCSC Early Warning



Part 3B

Response to Ransomware



Rob Tillman
Hampshire County Council

Response

Ransomware Event

- Indicators
- Invoking the response plan
- Paying the ransom?

Recovery

- Verify Backups
- Recovery key factors



Ransomware event - Indicators



Respond - 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'll be paying criminal groups
- You're more likely to be targeted in future
- **They still have 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/>

Respond - Invocation of response plan

- Follow your plan, tick off the steps as you progress through it.
- Consider incident response specialists to assist.
- Ask for help. Talk to initiatives such as Project Knapweed.
- Undertake Investigation, check for indicators of compromise



Key questions

- What is the impact – do we need to pay the ransom
- Do we need to delay recovery to protect evidence

Respond – Verify the backups

Verify your offline backups

- Ensure they don't show signs of compromise.

Check restored data

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



Key factors for recovery

- Ensure the entry point is identified.
- Rebuild.
- Restore (check restored data).
- Change every password in the school.
- Communicate.



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 team.
3. Treat it as a continuous improvement programme, train your staff every month.
4. Do the NCSC baseline work.
5. Fill out the DfE RPA template.
6. Your data is vital. **Back it up**, make it safe.
7. Use multi factor authentication on **everything** you can access over the internet.
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 address below

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

Thank you!

Useful links

Baseline NCSC Guidance

<https://www.ncsc.gov.uk/cyberaware/actionplan>

Response and Continuity Plan Guidance

<https://www.rpaclaimforms.co.uk/wp-content/uploads/2022/03/RPA-Cyber-Response-Plan-Template-V1.0.pdf>

<https://educationdatahub.org.uk/cyber-resilience/>

- <https://educationdatahub.org.uk/resources/incident-reporting-and-contact-template/>
- <https://educationdatahub.org.uk/resources/disaster-recovery-procedure-and-plan/>

<https://ransomware.org/how-to-prevent-ransomware/creating-disaster-recovery-and-incident-response-plans/>

User training guidance

<https://www.ncsc.gov.uk/information/cyber-security-training-schools>

<https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>

<https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>

Useful links

Prevent

<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>

<https://www.ncsc.gov.uk/guidance/principles-for-ransomware-resistant-cloud-backups>

Incident Response guidance

https://educationdatahub.org.uk/wp-content/uploads/NCSC_Incident_response.pdf

<https://learn.microsoft.com/en-us/security/ransomware/protect-against-ransomware-phase1>

Useful links

NCSC Guidance

<https://www.ncsc.gov.uk>

<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/files/Ransomware%20what%20you%20need%20to%20know.pdf)

<https://www.ncsc.gov.uk/collection/10-steps>

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>