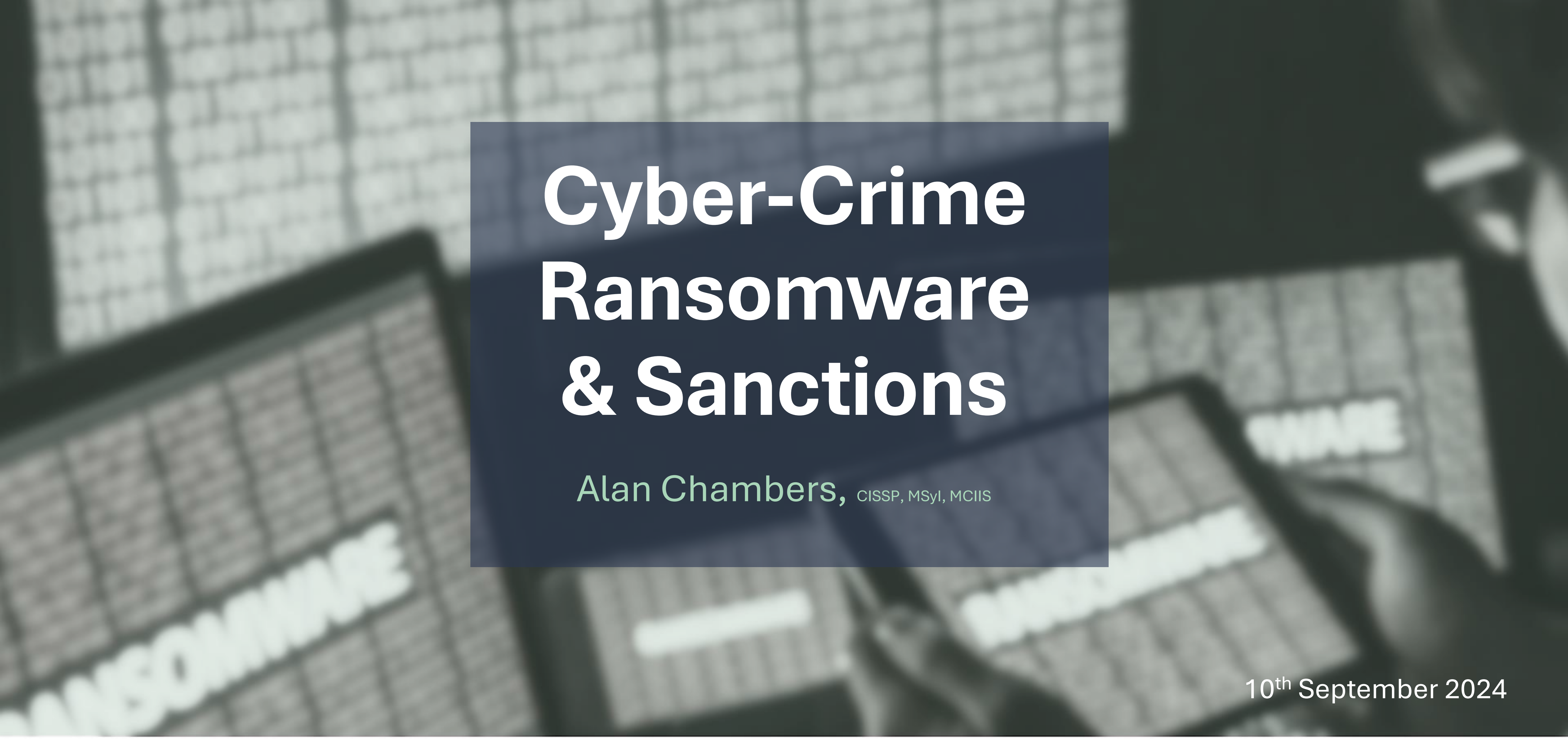


Cyber-Crime Ransomware & Sanctions

Alan Chambers, CISSP, MSyI, MCIIS

10th September 2024

Isle of Man Government
Reiltys Ellan Vannin

Isle of Man COUNTERING FINANCIAL CRIME
An all-Island approach

CSC Cyber Security Centre for the Isle of Man

information commissioner
Barrantagh Fysseree

Cabinet Office
Oik Coonceil ny Shirveishee

Department of Home Affairs
Rheynn Cooishyn Sthie

Introduction

What is Cybercrime?

Illegal activities conducted via the internet or other digital means.

Examples:

Hacking, identity theft, phishing, and ransomware attacks.

What is Ransomware?

- **Definition**: A type of malicious software designed to block access to a computer system until a sum of money is paid.

- **How it Works**: Encrypts files and demands a ransom for the decryption key.

- **Common Ransomware Strains**: Conti, Ryuk, Trickbot.

Risk to Businesses

Financial Loss: Costs associated with ransom payments, recovery, and downtime.

Data Breach: Loss of sensitive information.

Reputation Damage: Loss of customer trust and potential legal consequences.

Operational Disruption: Interruptions to business operations and services.

Case Studies

Example 1: **Attack on the Irish Health Service Executive (HSE)**

COSTA RICA
GOBIERNO DE LA REPÚBLICA

Example 2: **Costa Rican Government Ransomware Attack**

Attack on the Irish HSE

Date: 14th May, 2021

Attackers: Conti ransomware group

Attack on the HSE (2)

Impact:

- Total shutdown of HSE IT systems across Ireland
- Disruption of hospital services and appointment cancellations
- Data breaches involving medical and employee records
- Significant operational and financial impact on the healthcare system

Response:

- HSE took down IT systems to protect data
- Recovery involved extensive technical and operational efforts
- Demonstrated the need for improved cybersecurity measures and preparedness.

Costa Rican Government Attack

Date: April 17, 2022

Attackers: Conti ransomware group, followed by Hive ransomware group

CONTI

Hive Ransomware

Costa Rican Government attack (2)

COSTA RICA
GOBIERNO DE LA REPÚBLICA

Impact:

- Nearly 30 government institutions affected, including the Ministry of Finance and Social Security Fund
- Disruption of tax and customs systems, healthcare services, and other critical operations
- Estimated losses of $30 million per day due to operational disruptions
- Declaration of a national emergency by the Costa Rican government

Costa Rican Government attack (3)

Response:

- International assistance from the US, Israel, Spain, and Microsoft
- Implementation of emergency measures to restore services and enhance cybersecurity
- Ongoing efforts to address vulnerabilities and prevent future attacks.

Incidents closer to home

- Cayman National Bank
- STRIX
- Heron & Brearley / SPAR
- Hospitality
- Finance Sector
- Insurance Sector
- Legal Sector
- Public Sector (local authority)
- Charities
- Basically, anyone can be at risk of becoming a victim

Exploring the Evolving Tactics of Cyber Criminals

Sophistication of ransomware deployment techniques

Cyber criminals continually develop advanced tactics for deploying ransomware, leveraging encryption and social engineering to maximise impact.

Adaptation to security measures and law enforcement responses.

Criminals adapt to defensive measures and law enforcement responses, posing ongoing challenges to cyber-security professionals and authorities.

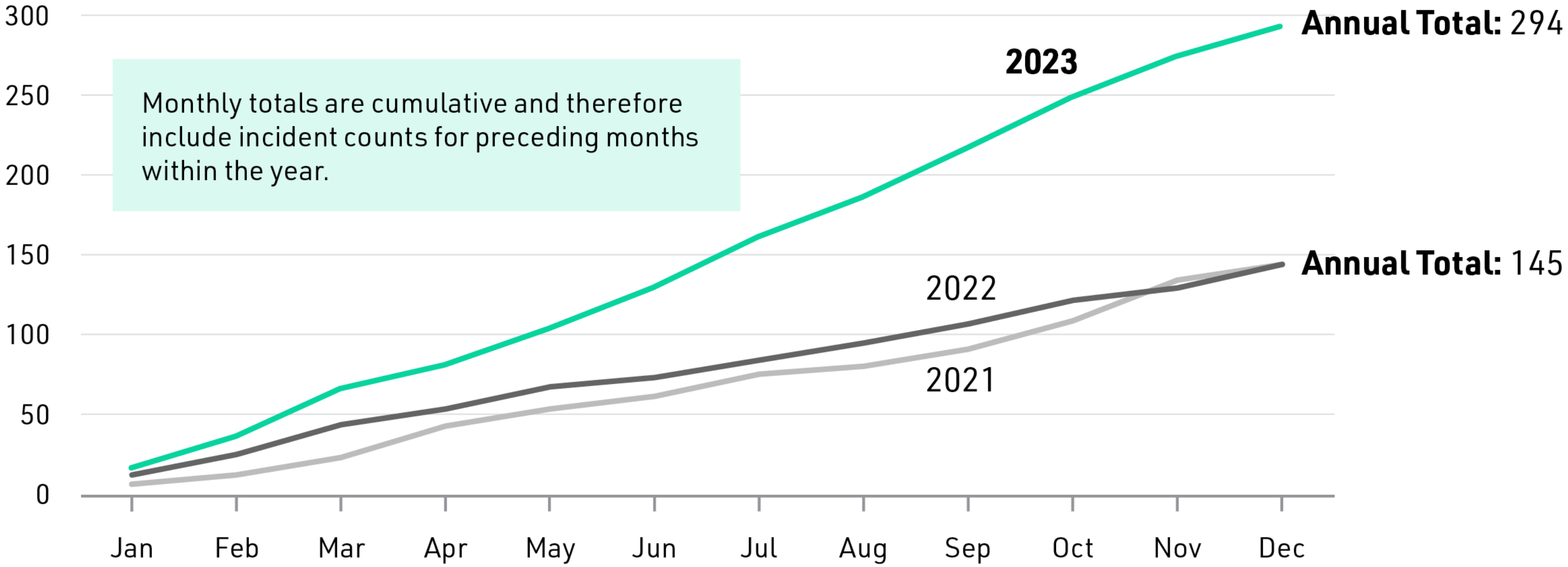
Emergence of double extortion strategies

Double extortion tactics, where cyber criminals threaten to leak sensitive data in addition to encrypting it, have become increasingly prevalent in ransomware attacks.

Exploitation of global events and vulnerabilities

Cyber criminals exploit global events and vulnerabilities such as the COVID-19 pandemic and the Crowdstrike outage, to launch targeted ransomware campaigns with heightened success rates.

A Significant Increase in Ransomware Incidents



Monthly totals are cumulative and therefore include incident counts for preceding months within the year.

Source: Data obtained by the National Crime Agency.

Global Efforts and Sanctions Against Ransomware

International Law Enforcement Collaboration

Global law enforcement agencies collaborate to combat ransomware, sharing intelligence and resources to identify and apprehend cyber criminals involved in ransomware activities

Economic Sanctions and Diplomatic Measures

Countries impose economic sanctions and diplomatic measures on nations or entities found to support or harbour ransomware operators, aiming to disrupt their infrastructure and funding sources.

Public-Private Partnerships and Cyber-Security Initiatives

Public and private sector partnerships develop cyber-security initiatives to strengthen defence capabilities, enhance incident response, and mitigate the impact of ransomware attacks.

Sanctions Against Cyber Criminals

Legal Sanctions

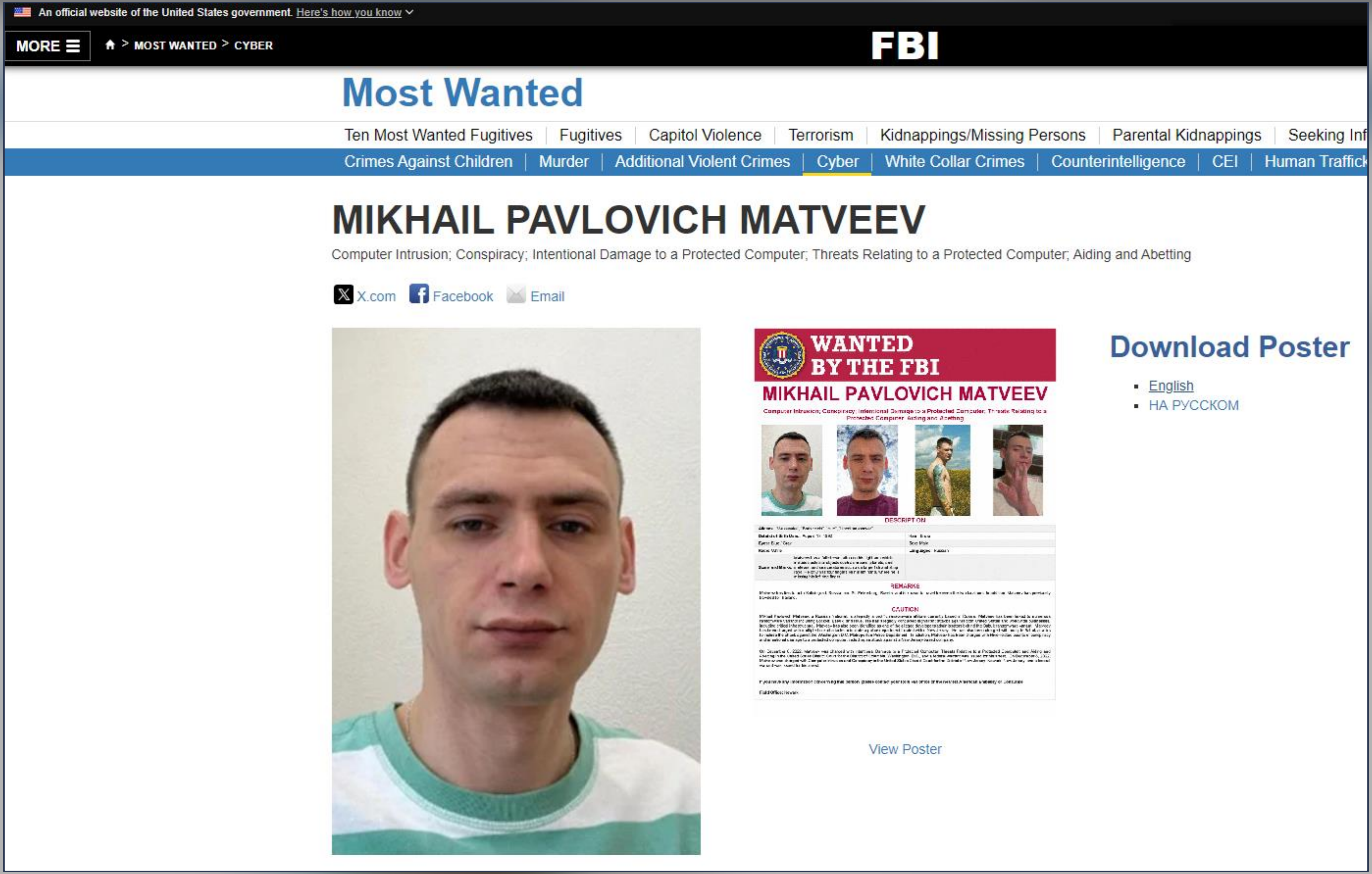
Countries impose legal sanctions such as fines, imprisonment and restrictions on cybercriminals involved in ransomware and cyberattacks.

Economic Penalties

Governments and international bodies impose economic sanctions on entities, blocking access to financial systems and assets.

International Co-operation

Global organisations collaborate to impose sanctions on state-sponsored cybercrime groups and criminal networks.



An official website of the United States government. Here's how you know

MORE ☰ 🏠 > MOST WANTED > CYBER

FBI

Most Wanted

Ten Most Wanted Fugitives | Fugitives | Capitol Violence | Terrorism | Kidnappings/Missing Persons | Parental Kidnappings | Seeking Inf

Crimes Against Children | Murder | Additional Violent Crimes | Cyber | White Collar Crimes | Counterintelligence | CEI | Human Traffick

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting

X.com Facebook Email

WANTED BY THE FBI

MIKHAIL PAVLOVICH MATVEEV

Computer Intrusion; Conspiracy; Intentional Damage to a Protected Computer; Threats Relating to a Protected Computer; Aiding and Abetting

DESCRIPTION

REMARKS

CAUTION

View Poster

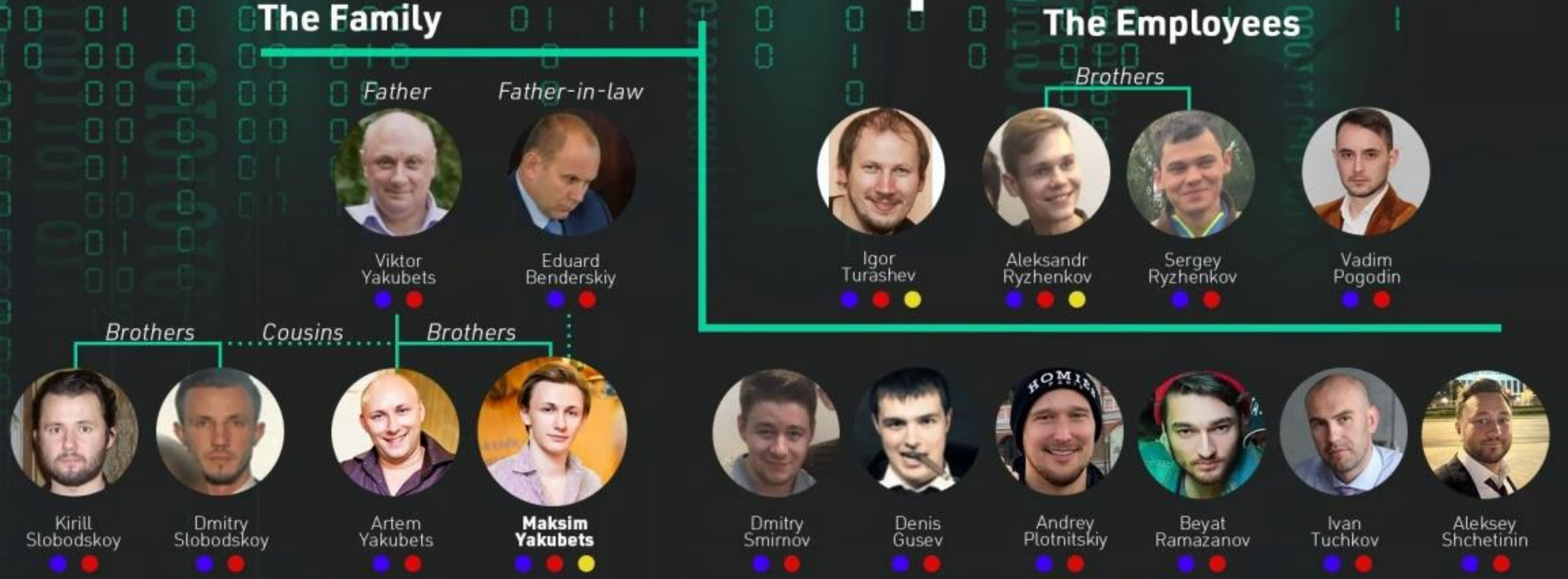
Download Poster

- English
- НА РУССКОМ

SANCTIONED

NCA
National Crime Agency

Evil Corp



The Family

Father
Viktor Yakubets
🔵 🔴

Father-in-law
Eduard Benderskiy
🔵 🔴

Brothers

Kirill Slobodskoy
🔵 🔴

Dmitry Slobodskoy
🔵 🔴

Cousins

Brothers

Artem Yakubets
🔵 🔴

Maksim Yakubets
🔵 🔴 🟡

The Employees

Igor Turashev
🔵 🔴 🟡

Brothers

Aleksandr Ryzhenkov
🔵 🔴 🟡

Sergey Ryzhenkov
🔵 🔴

Vadim Pogodin
🔵 🔴

Dmitry Smirnov
🔵 🔴

Denis Gusev
🔵 🔴

Andrey Plotnitskiy
🔵 🔴

Beyat Ramazanov
🔵 🔴

Ivan Tuchkov
🔵 🔴

Aleksey Shchetinin
🔵 🔴

Sanctions:

🔵 **United Kingdom** 🔴 **United States** 🟡 **Australia**

Legal Implications of Paying a Ransom

Paying a ransom to a designated person (DP) who is under international sanctions can have serious legal implications.

1. **Criminal Offence**: Making payments to individuals or entities under sanctions is generally prohibited and can be considered a criminal offence.

2. **Civil and Criminal Penalties**: Violating financial sanctions can result in severe penalties, including hefty fines and imprisonment.

3. **Regulatory Scrutiny**: Organisations that make such payments may come under intense scrutiny from regulatory bodies.

4. **Reputational Damage**: Beyond legal consequences, paying a ransom to a sanctioned entity can severely damage an organisation’s reputation, leading to a loss of customer trust and potential business losses.

Legal Implications of Paying a Ransom (2)

Mitigating Factors: Regulatory bodies may consider mitigating factors, such as whether the organisation took steps to avoid the payment or reported the incident promptly.

However, these factors do not guarantee leniency.

It’s crucial for organisations to consult legal experts and follow regulatory guidelines when dealing with ransomware attacks to avoid breaching international sanctions.

Mitigation Strategies

Cybersecurity Measures

Regular updates, backups, and employee training.

Incident Response Plan

Steps to take in the event of a ransomware attack.

Legal Consultation

Importance of consulting legal experts before considering ransom demands

Preventative Measures Against Ransomware

Regular Software Updates

Ensure all software and systems are up to date with the latest security patches.

Data Backups

Regularly back up data and store it offline or in a secure cloud service.

Employee Training

Educate employees about phishing attacks and safe online practices.

Use of Antivirus and Anti-Malware

Install and regularly update antivirus and anti-malware software.

Preventative Measures Against Ransomware (2)

Network Segmentation
Divide the network into segments to limit the spread of ransomware

Access Controls
Implement strict access controls and use multi-factor authentication (MFA).

Incident Response Plan
Develop and regularly update an incident response plan.

Challenges and Future Outlook

Challenges in Cybercrime

Law enforcement faces difficulties due to the anonymous and borderless nature of cybercrime, alongside constantly evolving tactics by cybercriminals.

Future Trends

Predicted increase in ransomware-as-a-service (RaaS), Ai-enhanced cyberattacks, and more sophisticated cybersecurity technologies.

Innovation in Defence

Advances in AI and machine learning are expected to improve cybersecurity, helping to detect and counteract cyber threats more effectively.

Conclusion

1. Seek professional help to minimise the damage and impact
2. **Do not** pay ransom under any circumstances

Q & A

Cyber@gov.im 685557

https://csc.gov.im