TLP:CLEAR

Ransomware Insights:
Quick Tips to Keep Your Data Safe in 30 min

Cyber Tips Webinar – 03 April 2025

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Intro

- Topic of today: **Ransomware**
- Topic of the next Cyber Tips Webinar: **Incident handling**
- Q&A
- Expert: **John Fokker**, Head of Threat Intelligence at Trellix

Understanding ransomware

- Definition: "*Ransomware is a type of attack where threat actors take **control of a target's assets** and demand a **ransom** in exchange for the return of the asset's **availability and confidentiality***"
- Core threat actor actions on assets: **LEDS matrix**
  - **L**ock – **E**ncrypt – **D**elete – **S**teal (leak)
- Also see: atwork.safeonweb.be/tools-resources/ransomware

Source: ENISA's 'Threat Landscape for Ransomware Attacks' report, July 2022

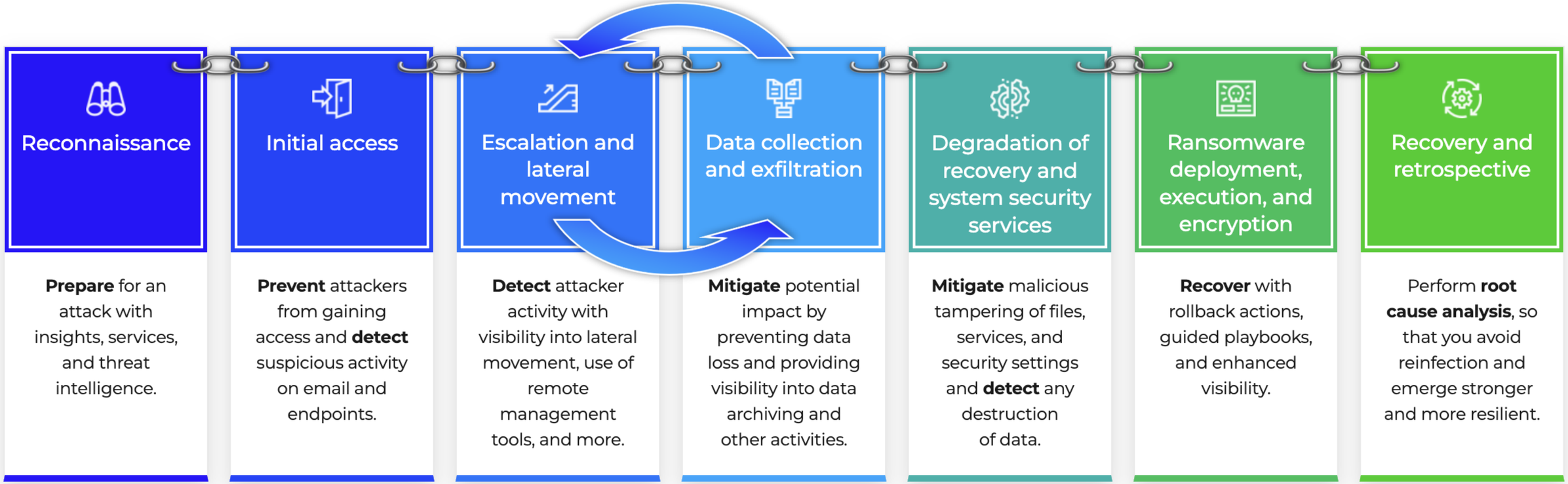
Impact

- **Financial loss**
  - Ransom (if paid) — *for 2023 the average ask was $4,321,880 * (for victims that had data encrypted)*
  - Recovery cost — *for 2023 a mean cost of $2.73M was reported to recover from a ransomware attack **
  - Regulatory fines
  - Business interruption loss
- **Operational disruption**
- **Reputational damage**

* Source: Sophos. 'The State of Ransomware 2024' (numbers for 2023, reported in 2024)

Ransomware attack chain

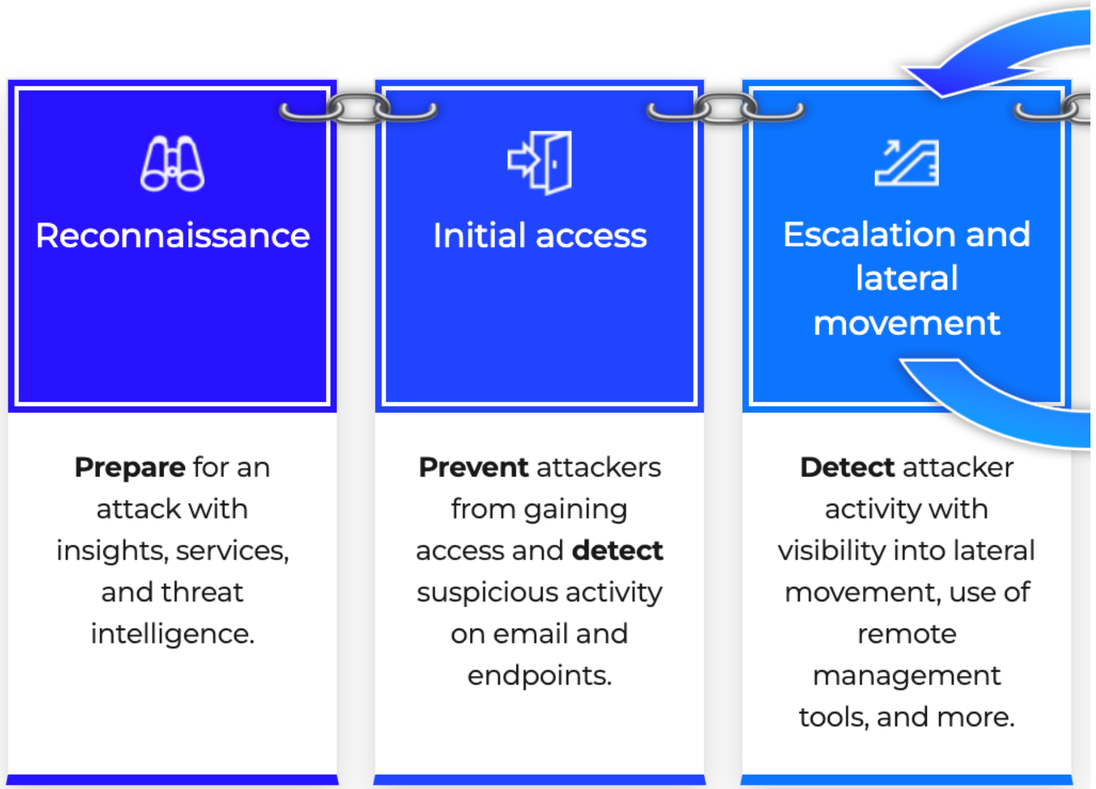
CENTRE FOR CYBERSECURITY BELGIUM



Source: Trellix (www.trellix.com/solutions/ransomware/)

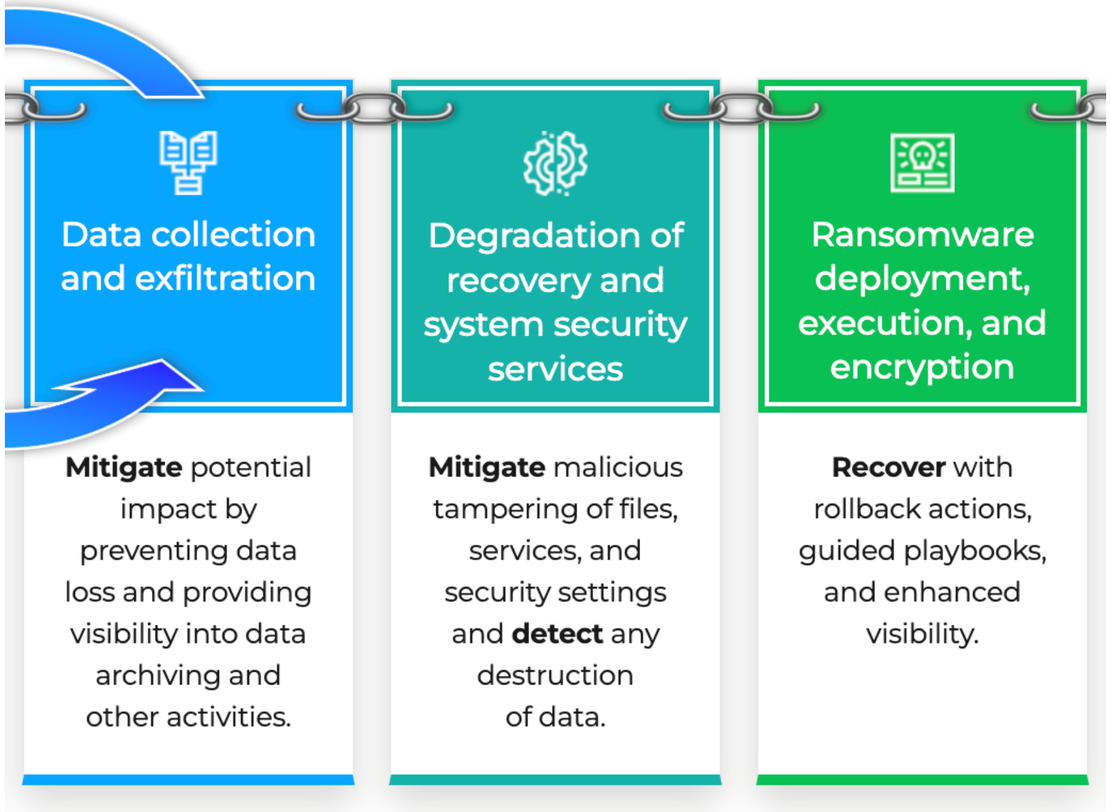
Prevention tips 1/2

- **Secure against scanning** (web-facing infrastructure)
- **Secure access** to your accounts (disable RDP, use MFA)
- **Protect against vulnerabilities** (patch management)
- **Protect against malware** (anti-malware, phishing awareness)



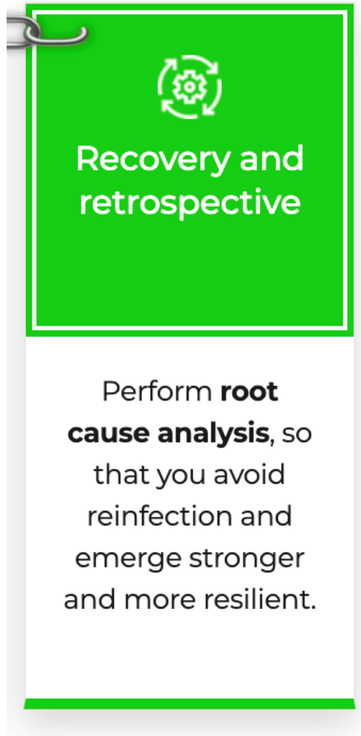
Prevention tips 2/2

- **Monitor** suspicious use of non-malicious tools and LOLBins
- **Monitor** data storage, file transfer and file modification activity
- **Encrypt** your sensitive data, both at rest and in transfer
- **Backup** your data and keep



Preparation tips

- The question is **not if** you will be hacked, **but when**
- Prepare an **Incident Response plan** and **test it**
- Prepare a **Business Continuity plan**



Source: https://ccb.belgium.be/sites/default/files/cybersecurity-incident-management-guide-EN.pdf

Remediation tips

CENTRE FOR CYBERSECURITY BELGIUM

- **Keep calm**
- **Isolate infected resources** from the network
- Follow your up-to-date cyber **Incident Response** (IR) and **Business Continuity** (BC) **plans**
- **Report** to your national CERT and to the police
  - CCB: notif.safeonweb.be (preferred) or via email at incident@ccb.belgium.be or call us at +32 (0)2 501 05 60
- CCB's advice: **don't pay the ransom**

Upcoming Webinars

Quarterly Cyber Threat Report (QCTR) event

- 25 April 2025 – 2.00-4.00 PM CEST

2025 EU MITRE ATT&CK Community Workshop (Hybrid)

- 15 May – full day

Cyber Tips webinar: Incident Handling

- 19 June 2025 – 3.00-3.30 PM CEST

What would you like to learn about?

Make yourself heard!

Give us your feedback and ideas:

- In the **chat**
- Via email at **info@ccb.belgium.be**

Did you know…

…that we have interesting vacancies?

Scan the QR code and discover our job offers for you.

CENTRE FOR CYBERSECURITY BELGIUM

Questions?

Ask away in the Q&A section!

Further questions can be sent to info@ccb.belgium.be

Resources I

Article with best practices on how to protect from a ransomware attack

- EN: https://atwork.safeonweb.be/tools-resources/ransomware
- FR: https://atwork.safeonweb.be/fr/tools-resources/ransomware
- NL: https://atwork.safeonweb.be/nl/tools-resources/ransomware

Guide 'How to respond to a ransomware attack in 12 steps'

- EN: https://ccb.belgium.be/recent-news-tips-and-warning/how-respond-ransomware-attack-12-steps
- FR: https://ccb.belgium.be/fr/recent-news-tips-and-warning/comment-repondre-une-attaque-par-ransomware-en-12-etapes
- NL: https://ccb.belgium.be/nl/recent-news-tips-and-warning/hoe-reageren-op-een-ransomware-aanval-12-stappen

Resources II

Blog by Trellix about Decoding the DNA of Ransomware Attacks: Unveiling the Anatomy Behind the Threat

- EN: https://www.trellix.com/blogs/research/decoding-the-dna-of-ransomware-attacks/

Blog by Trellix about the Hidden Story of Ransomware Victims – They're Not Who You Think

- EN: https://www.trellix.com/blogs/research/uncover-the-hidden-story-of-ransomware-victims/