Estimating the Carbon Footprint of Cyberattacks: *The Ransomware Case*

UQAC
Université du Québec à Chicoutimi

Fehmi Jaafar (fehmi.jaafar@uqac.ca), **Jean Decian** (jean.decian1@uqac.ca)
Department of Computer Science and Mathematics
University of Quebec at Chicoutimi

Introduction

Rise in Cybersecurity Threats

- More than double since 2020

Impact

- Mainly Financial and Operational
- Environmental largely unknown

Research Goals

- How can the carbon footprint of cyberattacks be quantified?
- What is the carbon footprint of ransomware attacks?
- How does the carbon footprint of ransomware compare with other energy-consuming activities?

Background

Carbon Footprint

Total amount of greenhouse gas emissions produced, both directly and indirectly

Ransomware

Malware that encrypts a target's data to demand a ransom in exchange for releasing the data

$$317.6\ million$$
$$= 5.24\%$$

Lifecycle of a Ransomware

- Initial access
- Consolidation and preparation
- Impact on target

Ransomware Core Actions

- **L**: Lock
- **E**: Encrypt
- **D**: Delete
- **S**: Steal

Cryptojacking

When an attacker hijacks the computer resources of a victim to generate cryptocurrencies

$$1.06\ billion$$
$$+659\%$$

Proposed Approach: CyberAttack Carbon Footprint (CACF)

$$CACF = C * U$$

Where:

- **C**: Sums of all emissions per unit
- **U**: Number of units

$$C = O + M + T$$

Where:

- **O (Operational Emissions)**: Emissions during the running of the software
- **M (Embodied Emissions)**: Emissions from the hardware production and utilization
- **T (Transfer Emissions)**: Emissions during data transfer

$$\boxed{CACF = (O + M + T) * U}$$

$$O = P * TiR * I$$

Where:

- **P**: Total Power consumed by the hardware
- **TiR**: Time Reserved by the software
- **I**: Carbon Intensity

$$M = TE * \frac{TiR}{EL} * \frac{RR}{ToR}$$

Where:

- **TE**: Total Embodied Emissions
- **TiR**: Time Reserved by the software
- **EL**: Expected Lifespan
- **RR**: Resources reserved by the software on the hardware
- **ToR**: Total resources on the hardware

$$T = B * I * E_T * N$$

Where:

- **B**: Bytes transferred
- **I**: Carbon Intensity
- E_T: Energy to transfer one byte
- **N**: Number of directions in which data are transferred

Results: The Ransomware Case

Estimated Carbon Emissions per Ransomware

Embodied Emissions (M)

- $TE = 3.93 * 10^5\ gCO_2eq$
- $EL = 35064\ h$
- $RR = ToR = 1$

$$M = 76\ gCO_2eq$$

Operational Emissions (O)

- $TiR = 6.8\ h$
- $P_O = 50 * 10^{-3}\ kW$
- $I = 481\ gCO_2eq/kwh$

$$O = 200\ gCO_2eq$$

Transfer Emissions (T)

- $B = 518 * 10^9\ bytes$
- $I = 481\ gCO_2eq/kwh$
- $E_T = 2.91 * 10^{-10}\ kwh/byte$
- $N = 2$

$$T = 145\ kgCO_2eq$$

Carbon Emissions for Ransomware Activities

$$C = 145\ kgCO_2eq/ransomware$$

- 317.6 million ransomware attacks recorded by one service provider
- 70% of ransomware attacks result in data encryption

$$\boxed{CACF_{Ransomware} = 32\ MtCO_2eq}$$

Discussion

Cybercrime are underreported

5% to 10% of cybercrime are reported.

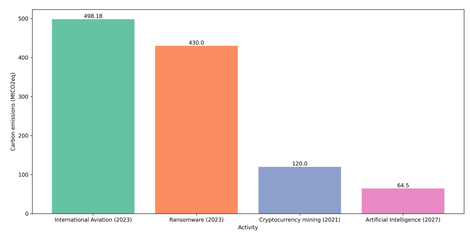
$$\boxed{430\ MtCO_2eq}$$

Comparison with G7 Countries

Rank	Country	Total 2023 GHG Emissions ($MtCO_2eq$)
2	United States	5960.80
7	Japan	1041.01
10	Canada	747.68
12	Germany	681.81
	Ransomware	430
20	France and Monaco	385.52
22	United Kingdom	379.32
23	Italy, San Marino and the Holy See	374.12

Comparison with other activities

Activities	Total GHG Emissions ($MtCO_2eq$)
International Aviation (2023)	498.18
Ransomware (2023)	430
Cryptocurreny mining (2021)	120
Artificial Intelligence (2017)	64.5



Conclusion

- Illustrates the substantial environmental impact of ransomware activities
- Proposed a formula for estimating the carbon footprint of cyberattacks
- Ransomware activities surpasses Cryptocurrency mining and Artificial Intelligence

References

Introduction

- Natalucci, Qureshi & Suntheim, 2024

Background

- CERT NZ, n.d.
- ENISA, 2022
- SonicWall Inc, 2024

Proposed Approach: CyberAttack Carbon Footprint (CACF)

- Green Software Foundation, n.d.

Results: The Ransomware Case

- ENISA, 2022
- European Commission Joint Research Center, 2024
- Marsh, 2024
- Our World in Data, 2024
- SonicWall Inc, 2024
- Sophos, 2024
- Splunk SURGe, 2022
- The Shift Project, 2019

Discussion

- European Commission Joint Research Center, 2024
- Hebous & Vernon-Lin, 2023
- Office of the Auditor General of Canada Government of Canada, 2024
- Vries, 2023