TLP:CLEAR

CENTRE FOR
CYBERSECURITY
BELGIUM

RESEARCH REPORT

UNCOVERING PATTERNS BETWEEN GDP SIZE AND RANSOMWARE GANGS' CHOICE OF TARGETS

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: 01 Feb 2024
Version: 1.0 EN
Author: Centre for Cybersecurity Belgium (CCB)

Target audience:
General public

Permitted distribution of TLP:CLEAR:
No limits to disclosure, recipients can spread this freely outside their organizations.
More information: https://www.first.org/tlp/

Table of Contents

EXECUTIVE SUMMARY

Ransomware is the single biggest threat to organizations online. Year on year, the number of ransomware cases increases. The average ransom price reaches in the hundreds of thousands of euros. While any organization anywhere can fall victim to ransomware, this report looks into the mechanics behind targeting. This study is based on around 14.000 records coming from data collected by the company Trellix as well as data scrapped from data leak extortion sites operated by ransomware groups. We used gross domestic product (GDP) calculated by the World Bank to measure a nation's wealth.

By looking at who became victims, we uncovered geographical and economic patterns underlying ransomware operations.

- There is a **positive relationship** between GDP and the number of ransomware incidents. 89% of the variation of ransomware victims can be explained by GDP in Europe, 72% in Asia.
- GDP is the **stronger indicator** in comparison to population.
- Europe and North America concentrate **80%** of victims. The **United States** is by far the country with the most ransomware victims. Belgium is neither over nor under attacked in relation to its GDP size.
- The number of ransomware victims more than **doubled** since 2021.
- Between 2021 and mid-2023, ransomware actors have been mainly targeting the same sectors.

PRELIMINARY NOTE ON THE DATASETS

It is very difficult to obtain reliable data on ransomware. **Visibility over ransomware is limited** to what is publicly available as observed on data leak sites and posts on the dark net; or what vendors and incident response companies are willing to publish online. Partial visibility is the reason why this report was created by looking at the organizations who were victims of ransomware. **Entities who successfully fended off ransomware attacks are not in scope.**

The following data is only a subset of the true extent of ransomware threats. The exact proportion that public ransomware data represents in comparison with **the total amount of ransomware is unknown**. In CCB's experience, there are many times more cases of ransomware reported to the Centre for Cybersecurity Belgium (CCB) by organizations than there are mentions on extortion sites. On average, one of our CTI platforms finds 5.5 cases of ransomware per quarter, whereas there was an average of 23 cases reported to CCB per quarter in 2022. **To gain additional visibility over ransomware internationally, CCB welcomes any information sharing from other national CSIRTs, law enforcement agencies or private companies.**

For this report, CCB relied primarily on **two datasets**. The dataset shared by Trellix contained a combination of records from **sensor data, incident response and open sources**. The other dataset consists of data scrapped from **public data leak extortion sites (DLS sites)**. Both datasets span the period January 2021 until August 2023.[1]

As filtering accurately was difficult and so as to avoid potential duplicates, the datasets were not combined. The same statistical operations were run on both datasets to allow for comparisons.

This analysis focuses on absolute numbers over a certain period of time. Therefore, in order to draw relevant conclusions from the datasets, we applied data transformation to mitigate the effects of non-normal distribution. More precisely, we used the generalized linear model with a Poisson distribution.

There are **intelligence gaps** that need to be highlighted.

- Typically, only ransomware victims who refused to pay end up on a ransomware gang's data leak extortion site (DLS). Organizations that paid the ransom are therefore most likely not accounted for in the datasets used in this study.
- Some ransomware groups do not operate DLS websites.
- It is impossible for our partners to be tracking the DLS websites of every single ransomware group.
- Concerning Trellix's data, no single company holds a representative view on ransomware. Part of their data comes from the various incidents they have been called upon to resolve. Their visibility is limited to where they operate. A significant part of Trellix's operations takes place in the United States which could partly explain the immense number of victims

[1] Additional data was collected from public sources to maintain quarterly visibility in figures 7 and 8.

reported there.
In addition, 27% of the records CCB received from Trellix were not mapped to any particular country. As a result, they are not included in this study.

CCB hopes to receive additional data in the future that could help fill in intelligence gaps to further strengthen the analysis and conclusions below.

CALL FOR COLLABORATION

Establishing a reliable dataset was a difficult and painstaking task. CCB is aware that the quality of the analysis and the conclusions that were drawn hinges on its ability to gather sufficient data. We approached partners who had visibility internationally. We would like to extend our thanks to our partners Trellix and INTEL471 for their collaboration.

While we were able to collect close to 14.000 records, we are aware that intelligence gaps remain. With more information, we could periodically review the extent of our knowledge on the state of ransomware globally.

This is why CCB is looking to expand collaboration with reliable partners. With the help of fellow experts, we look forward to thinking together and using additional sources in order to improve our datasets and our analyzes.

---

*If you are a researcher or work for an organization with a strong focus on ransomware and **if you have information on ransomware incidents** that you could share (such as modus operandi, number of incidents, ransom amount, underground monitoring,…), **please consider participating in this initiative**. Simply send us an email at intelligence@ccb.belgium.be to get the conversation started.*

ANALYSIS

Link between GDP size and number of ransomware victims

There is a **positive relationship** between a country's wealth as measured by GDP and the number of ransomware victims. The distribution of victims as exemplified in figures 1.1 and 1.2 highlights three things:

- There is a general upward trend suggesting that **the higher the GDP, the higher the number of ransomware victims.**
- **The relationship between GDP and the number of ransomware victims is especially true for the region of Europe**. European countries that have more than 1 case of ransomware tend to align the most with the regression line. Other regions have more scattered data points. The United States stand out as a clear outlier.
- Some countries are little targeted by ransomware. This is the case for many African nations, as well as some European nations. A closer look into the breakdown of attacks shows that **small European states rarely appear as victims of ransomware**.

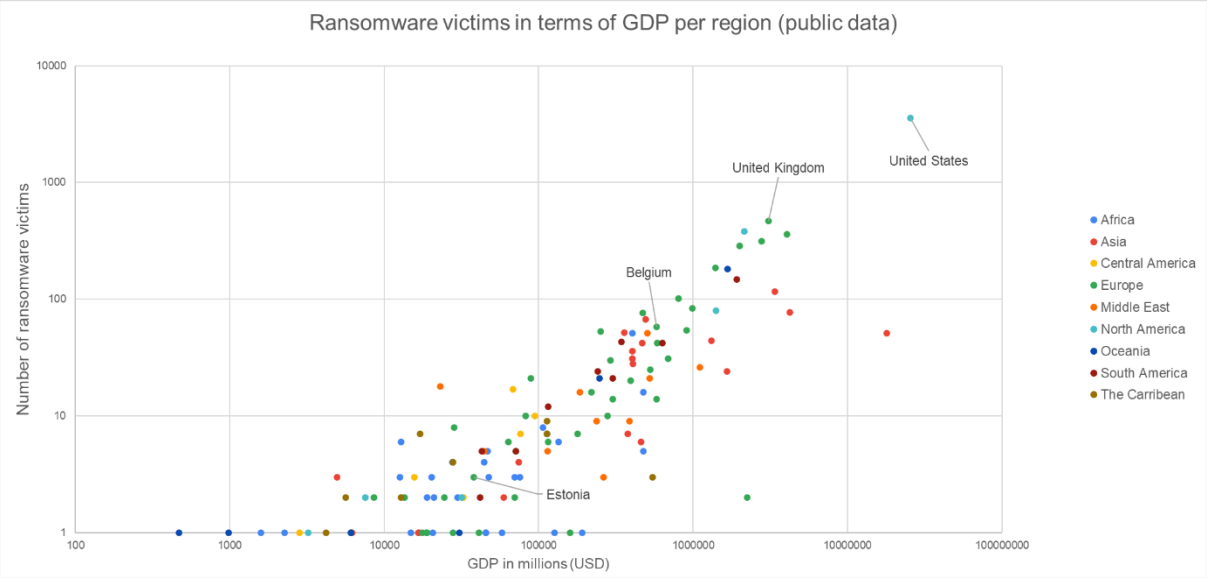


Figure 1.1 : Ransomware attacks (GDP to world regions) according to public DLS sites

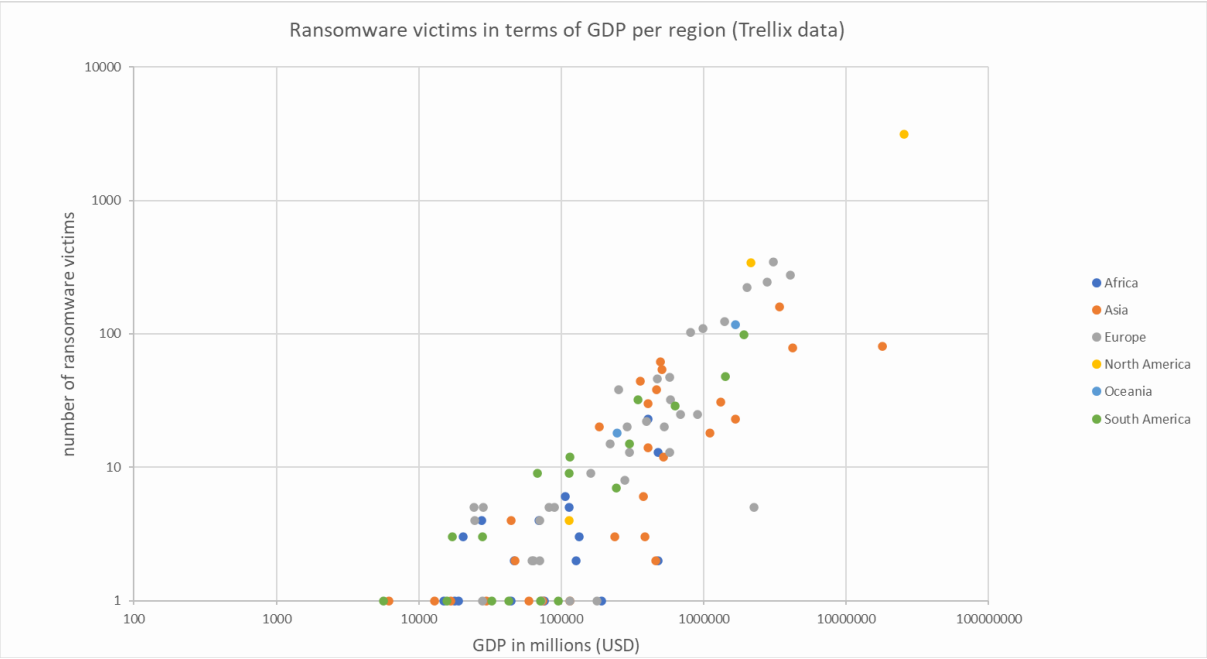
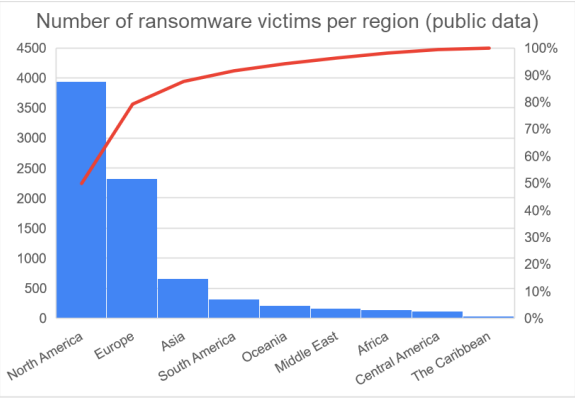


Figure 1.2 : Ransomware attacks (GDP to world region) according to data shared by Trellix

Ransomware attacks tend to be **concentrated in North America and Europe**, the world's wealthiest regions, who account for more than 80% of the total number of victims worldwide (Figures 2.1 and 2.2). The wealthiest countries tend to have more public-facing operational infrastructure and therefore a bigger attack surface.



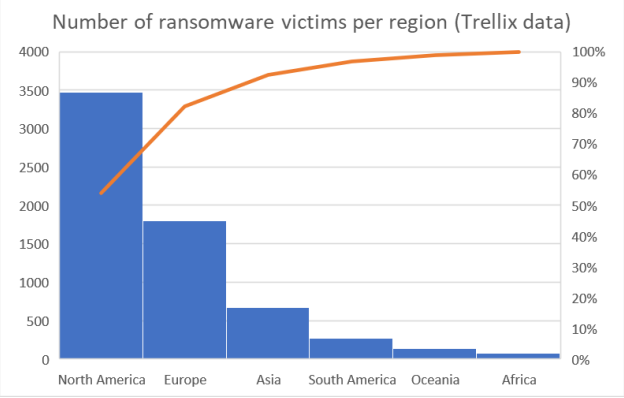


Figure 2.1 : Number of ransomware victims per region as derived from data posted on DLS websites.
Figure 2.2: Number of ransomware victims per region as shared by Trellix.

The 5 countries with the most ransomware victims are all located in North America or Europe (Figures 3.1 and 3.2).

Number of ransomware victims per country, January 2021 - August 2023 (Trellix data)		
Country	**Number of ransomware victims by country**	**Ransomware victims by country compared to the total number of victims worldwide (%)**
United States of America	3.125	47.9
United Kingdom	347	5.3
Canada	343	5.2
Germany	277	4.2
France	246	3.7
Italy	222	3.4
India	159	2.4
Spain	123	1.8
Australia	118	1.8
Netherlands	110	1.6

Figure 3.1 : Number of ransomware victims per country, 2021-2023 (Trellix data)

Number of ransomware victims per country, January 2021- September2023 (public data)		
Country	**Number of ransomware victims by country**	**Ransomware victims by country compared to the total number of victims worldwide (%)**
United States of America	3.383	44.8
United Kingdom	443	5.8
Canada	365	4.8
Germany	347	4.6
France	299	3.9
Italy	283	3.7
Spain	177	2.3
Australia	169	2.2
Brazil	140	1.8
India	116	1.5

Figure 3.2 : Number of ransomware victims per country, 2021-2023 (public data)

Western nations of the G7 in particular have the highest number of victims as exemplified in the maps below (Figures 4.1 and 4.2). It is plausible that ransomware actors show a preference for

targeting organizations in the richest Western countries. This finding agrees with a statement from a LockBit ransomware gang's spokesperson who stated that "it is in [the United States of America and the EU] that most of the world's richest companies are concentrated"[2]. In this case, it shows that **a company's location is a key factor in targeting because threat actors assume wealth based on it.**

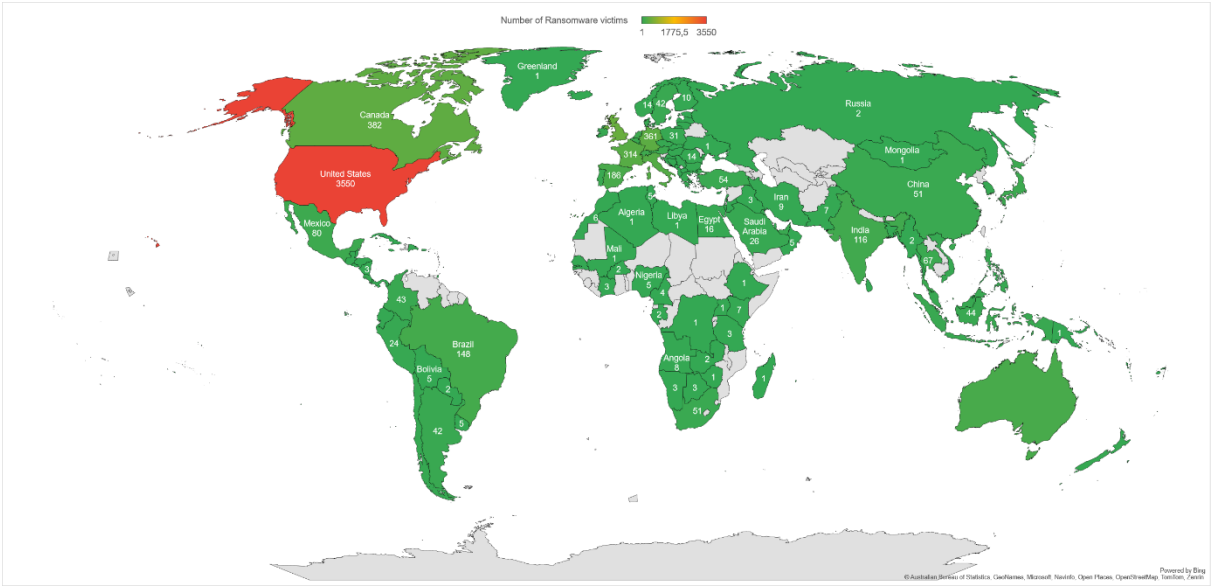


Figure 4.1 : Map of the world showing the number of ransomware victims per country, 2021-2023 (public data)

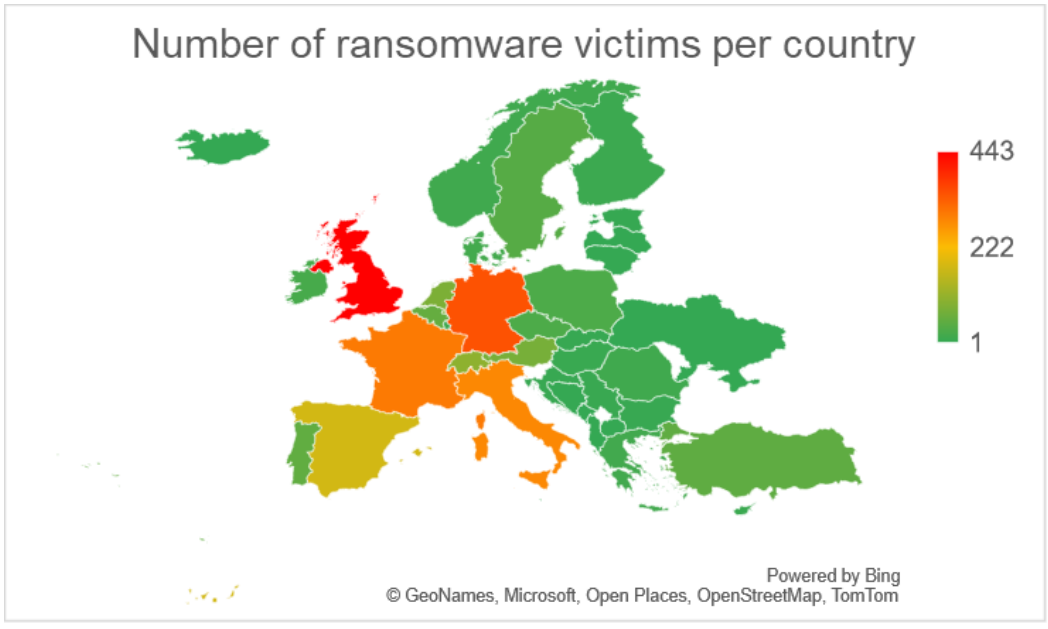


Figure 4.2 : Map of Europe showing the number of ransomware victims per country, 2021-2023 (public data)

[2] Unnamed author. "LockBit 2.0 Interview with Russian OSINT", Kelacyber.com, KELA Cyber, 24 August 2021, last accessed on 12 January 2024, https://www.kelacyber.com/lockbit-2-0-interview-with-russian-osint/

Macroeconomics matter most in Europe

To verify the assumption of a positive correlation between GDP size and the number of ransomware victims, CCB chose to focus on Europe and Asia. These are the two world regions for which CBB had the most data points[3].

For the purposes of this study, Europe does not include the **Russian Federation and Ukraine**. Both countries are outliers in this dataset: they have a medium GDP size but very few ransomware victims. Several ransomware groups have expressly or customarily barred their affiliates from using their software against organizations in the Commonwealth of Independent States (CIS). Excluding Ukraine and Russia from the model enhances the confidence level of the mathematical model.

Data transformation was applied on GDP so as to conform to model assumptions[4]. In this model based on public data, GDP can explain **89%** of the variations between the number of ransomware victims across different countries of Europe[5]. Similarly, in Asia, **72%** of the variation of ransomware victims can be explained by GDP[6].

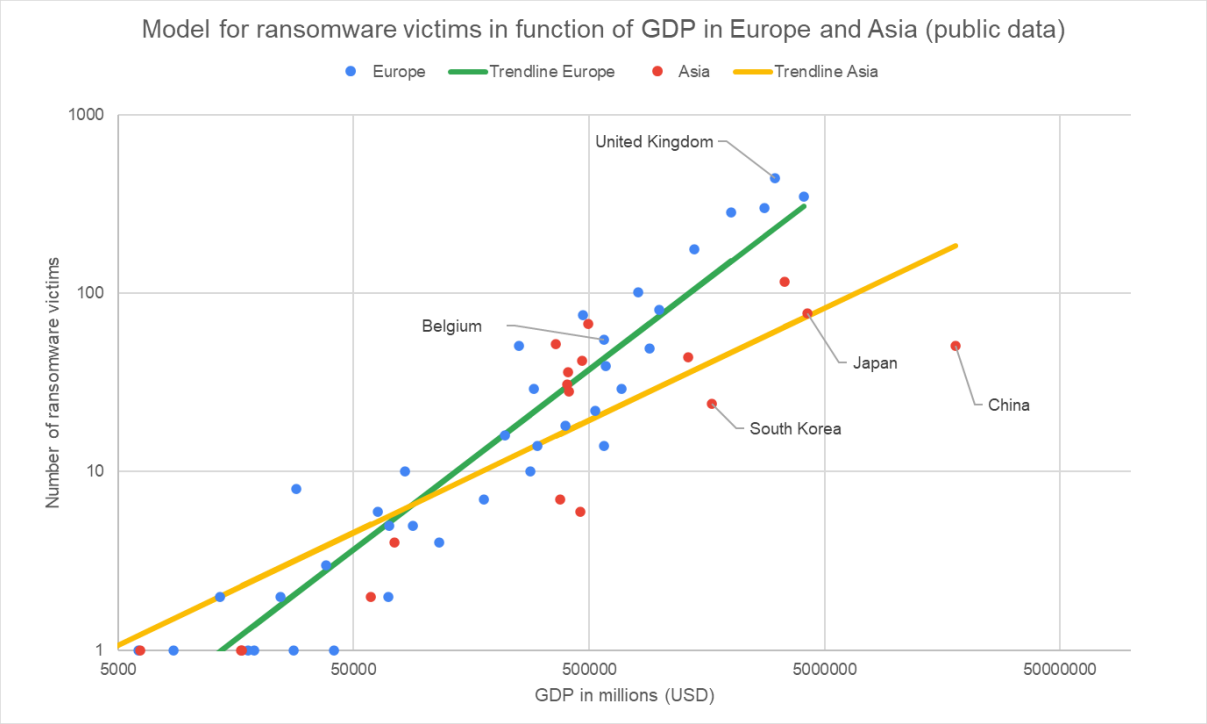


Figure 5 : CCB built this model that exemplifies the link between a country's wealth (as measured by GDP) and the prevalence of ransomware victims. Model built based on public data.[7]

[3] CCB chose not to consider building a model for North America despite having data points for many of its countries because the United States is a strong outlier.
[4] A Poisson regression was used to predict the frequency of an event.
[5] When using Trellix data and applying the same mathematical analysis, a similar result is reached: in this case, GDP explains 77% of the variations in number of ransomware victims in Europe.
[6] In this study using public data, the category Asia does not include the Middle East.
[7] In this graph, the trendlines appear to be straight lines. This is due to the close-up visualization. In fact, the trendlines are exponential.

In statistical analysis, variance represents the degree of spread of a dataset in relation to the mean. In this case, GDP is the predictor variable. In other words, **GDP is significantly correlated with the number of ransomware victims. GDP is the strongest studied indicator to explain why a given European or Asian country is targeted.** Other studied indicators include population size and GDP per capita.
However correlation is not causation. This finding cannot be understood to mean that 89% of ransomware attacks in Europe are due to GDP.

In this model (Figure 5), GDP is a stronger predictor in Europe than in Asia. Rich Asian nations account for a large chunk of the world's economy but have low ransomware attack numbers with respect to their economic size. **China** in particular, as well as **Japan** and **South Korea** have very few victims in comparison with the importance of their respective economies. China is the second world economy but ranks low in the top 30 most affected countries (13th according to Trellix data, 21st according to public data). Japan ranks 3rd in GDP and is only the 15th country with the most ransomware victims (public data).

Possible **hypotheses** include:

- **Language**, and the ability to understand and read non-Latin characters, could discourage non-domestic ransomware attackers from targeting these organizations. Not speaking the language makes crafting convincing phishing emails more difficult. What is more, in order to successfully reach its actions on objectives a threat actor would need to perform lateral movement. Without knowledge of the language, an actor might struggle knowing where and what is the valuable data they should exfiltrate.

- Asian economies historically developed around big **conglomerates** in the last 50 years. Large firms typically have dedicated cybersecurity staff and are therefore better protected against cyberattacks than smaller organizations[8].

However, there are significant **intelligence gaps** in the datasets for Asia and Africa. Only about a quarter of African countries are mapped in the public dataset. Similarly, there is public information on about half of Asian countries.

To sum up, GDP as an macroeconomic indicator sheds light on why some countries are more affected by ransomware than others. Pattern analysis shows that there are more ransomware victims in countries with a high GDP likely because ransomware groups assume wealth based on the size of a country's economy. This finding is especially true in Europe whereas GDP is a relevant yet less powerful indicator for other regions such as Asia. The filling of significant intelligence gaps, such as gaining visibility on ransomware payments, might give a different picture.

[8] The Japanese definition of small and medium businesses include companies of various sizes, with an upper limit between 100 to 500 employees, as explained in https://www.wipo.int/edocs/mdocs/aspac/en/wipo_ip_dev_tyo_09/wipo_ip_dev_tyo_09_ref_t7.pdf
In comparison, Belgium takes an upper limit of 250 employees, as illustrated in https://economie.fgov.be/fr/themes/entreprises/pme-et-independants-en/statistiques-relatives-aux-pme#:~:text=Qu'entend%2Don%20par%20petite,Carrefour%20des%20Entreprises%20(BCE). International comparisons around small and medium businesses are difficult to draw due to definitional differences.

Analysis of an outlier: the United States

The **United States** (USA) dominate the charts. Public data shows that a little under half of the world's ransomware victims are located in the USA. Similarly, the number of ransomware victims in the USA is 7.6 times the amount of the second most targeted country, the United Kingdom. The USA is somewhat of an outlier for being **disproportionately targeted** in comparison with the size of its economy.

There are **multiple hypotheses** that could shed light on this phenomenon:

- The USA has more ransomware victims because it has **overall in volume more businesses** than most other G7 countries, and therefore more potential victims[9].
- The prevalence of **online commerce** could play a role as well: organizations in the USA are compelled to have an online presence to satisfy a large share of their customers. Poor security practices with online resources could be used for initial access.
- It is also plausible that this high number is due to a **bias** in data collection. The organizations that provided the datasets are very active in the United States. In the case of Trellix, they confirmed that many of their engagements are purely domestic.
- A third hypothesis concerns **marketing**. As diverse ransomware groups compete against each other for market shares in this very profitable industry, they seek to establish dominance by gathering media attention. A wave of attacks against American companies are likely to be picked up by local, national and sometimes international media. This also has the added benefit of increasing the pressure put on victims to pay the ransom.
- A last hypothesis could be due to **geopolitical reasons**. The USA has been a major player in world politics in the last century. Affiliates and actors from certain countries might deliberately attack a country that they would perceive as offensive and imperialistic.

Link between population size and number of ransomware victims

In addition to researching the relationship between GDP and the number of ransomware victims, CCB investigated if population size was also a relevant indicator. Only about **45%** of the number of ransomware victims can be explained by a country's number of inhabitants (Figure 6). As a result, CCB dismisses population as a good indicator of ransomware targeting.

Ransomware groups are **financially-motivated**. They show a preference for **targeting countries based on their wealth rather than the size of their population.**

[9] The number of USA businesses was gathered from the United States Census Bureau's Statistics of U.S. Businesses (SUSB) latest study from 2021. The dataset is freely available at https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html

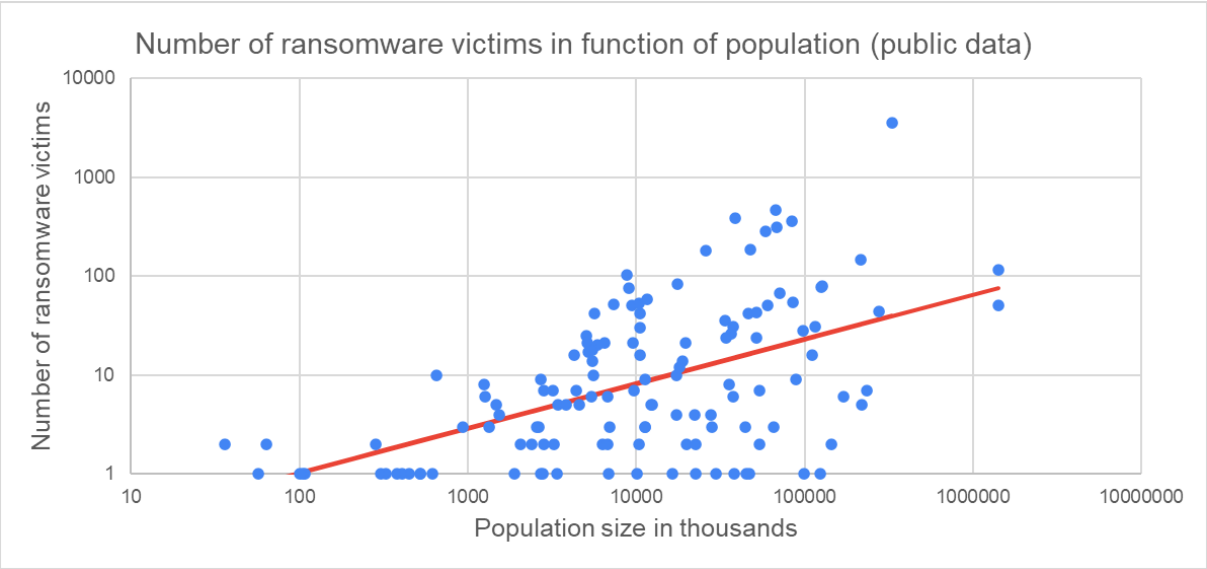


Figure 6 : Number of ransomware victims in function of population size (public data).

Ransomware trends between January 2021 and September 2023

An analysis of the public dataset from January 2021 until September 2023 shows **that the overall number of ransomware victims more than doubled in the time period.** In spite of a brief respite in 2022, **ransomware is a growing threat.**

There is a dip between Q1 and Q3 2022 (Figure 7), which corresponds to the early days of the Ukraine-Russia conflict. Many ransomware groups are Russophone. The collaboration between operators and affiliates that existed prior to the conflict was disrupted as political lines were redrawn and some actors possibly sent to fight with the army. The subsequent decrease and plateau could partly be explained by the necessary reorganization of the Russian-speaking ransomware ecosystem following the war. After reorganization, the number of ransomware victims skyrocketed.

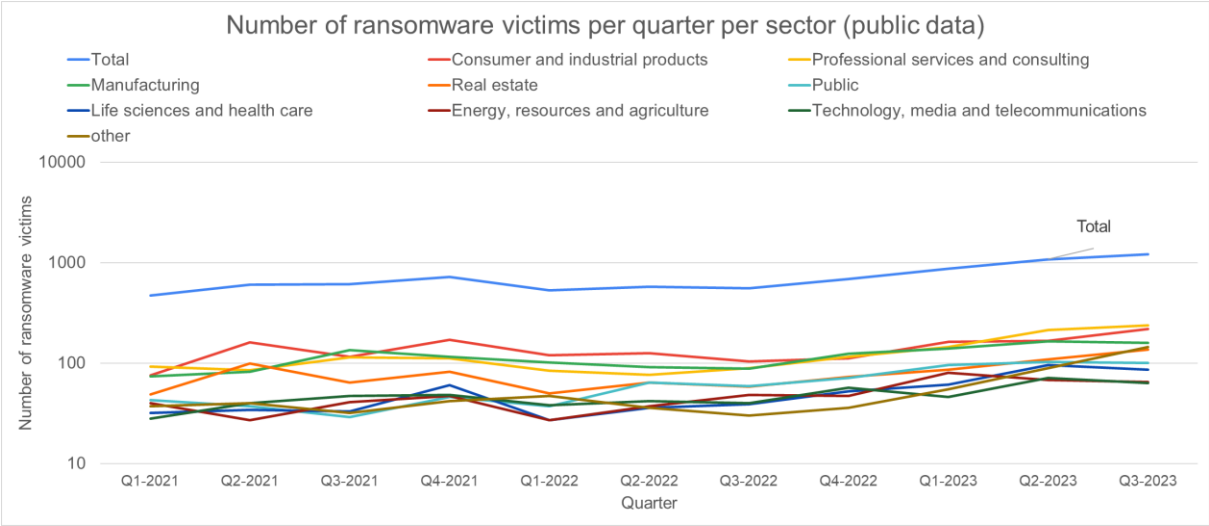


Figure 7: Number of ransomware victims per sector (public data)

Over the course of close to 3 years**, ransomware groups have not significantly changed their targeting**. Consumer and industrial products, manufacturing and professional services and consulting remain consistently the sectors with the largest amount of victims.

On the other hand, agriculture is little targeted. Agriculture is still a very manual sector. Where machines are needed, they are not necessarily connected to the internet. More surprisingly, energy is also among the least targeted sectors despite it being a crucial topic in the winter of 2023, with prices skyrocketing worldwide.

Several hypotheses could explain this:

- Energy is a critical sector that relies on specific equipment and protocols that differ from the technology used in other sectors. Attacking energy companies would **thus require additional sophistication** on the actors' part.
- Energy companies are typically big companies with **mature and dedicated cybersecurity teams** who have resources to tackle cyber threats.
- Energy is part of critical infrastructure and can lead to **law enforcement prosecution**. For example, in the aftermath of the ransomware attack on Colonial Pipeline, US law enforcement made it clear that attacking domestic critical infrastructure would lead to serious consequences. It is believed that Russia arrested the hackers responsible for this, and some of the ransom was taken back by law enforcement.[10] The risk of arrest and the prospect of not making money off an energy-focused heist might discourage some affiliates even when energy prices were at their highest.

[10] Matishak, Martin. "White House: Arrested Russian hacker was behind Colonial Pipeline attack", therecord.media, The Record, 14 Jan 2022, last accessed 21 December 2023, https://therecord.media/biden-official-one-of-arrested-russian-hackers-carried-out-the-colonial-pipeline-attack

- The energy sector is primarily interested in maintaining availability. However, ransomware gangs' techniques of data theft and extortion tend to impact confidentiality rather than availability.

Evolution of ransomware families

In terms of ransomware families, **LockBit** - both 2.0 and 3.0 - has been the most used ransomware strain between 2021 and mid-2023. The group claimed close to 25% of total victims worldwide according to DLS data. The graph illustrates when the group updated its ransomware software, causing the name to change from LockBit 2.0 to LockBit 3.0 In June 2022. The rise in the number of victims from **Cl0p** ransomware throughout 2023 can be linked to the group leveraging vulnerabilities in Fortra GoAnywhere (CVE-2023-0669)[11] and MOVEit Transfer (CVE-2023-34362)[12].

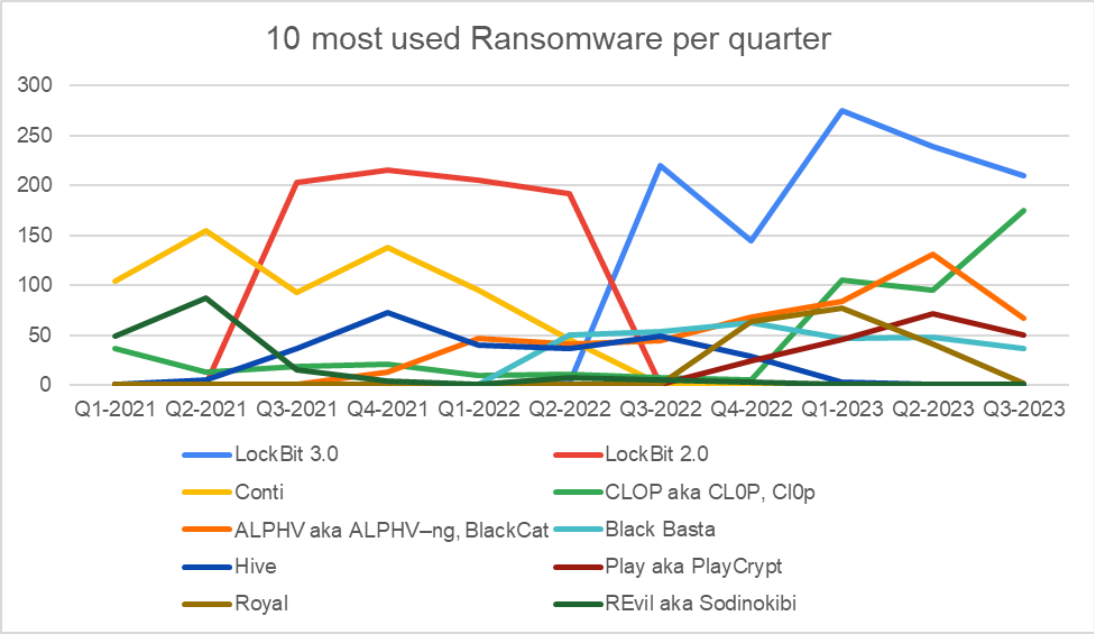


Figure 8 : Top 10 most used ransomware families (public data)

[11] Lakshmanan, Ravie. « Fortra Sheds Light on GoAnywhere MFT Zero-Day Exploit Used in Ransomware Attacks", TheHackNews.com, The Hacker News, April 20 2023, last accessed January 24 2024, https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html

[12] Unnamed author. « Cl0p Ups The Ante With Massive MOVEit Transfer Supply-Chain Exploit", Resecurity.com, Resecurity, August 23 2023, last accessed January 24 2024, https://www.resecurity.com/blog/article/cl0p-ups-the-ante-with-massive-moveit-transfer-supply-chain-exploit

Conclusion

Ransomware has been a **growing trend**. Between January 2021 and the end of summer 2023, the number of victims more than doubled. A study of the victims suggests that ransomware **threat actors show a preference for targeting organizations based in rich Western nations of North America and Europe**. **GDP is a strong indicator** of the number of ransomware victims for Europe but its relevance is somewhat more limited where other world regions are concerned.

The ransomware landscape has not significantly changed since 2021. LockBit remains the most significant player. The same sectors were targeted throughout although we do note an uptick in the professional services and consulting industry which shows the biggest increase since Q3 2022.

Geopolitics and economics affected the ransomware ecosystem for a limited amount of time. After a dip in activity following the start of the Ukraine-Russia war, activity picked up strongly again in Q4 2022. The rise in energy prices saw a limited increase in the targeting of this particular sector.

ABOUT THE CCB

The **Centre for Cybersecurity Belgium (CCB)** is the national authority for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the application of the Belgian cyber security strategy. Through optimal information exchange, companies, the government, providers of essential services and the population can protect themselves appropriately.

The Centre for Cybersecurity Belgium (CCB) was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

Disclaimer

This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations.
- are not necessarily exhaustive, precise, or up to date on all points.

Responsible editor

Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 18
1000 Brussels

Legal Depot

D/2024/14828/005