CyberPeace Institute

RANSOMWARE

Follow the Threat Actor

Geneva - 2025

October, 2025

Geneva, Switzerland

media@cyberpeaceinstitute.org

https://cyberpeaceinstitute.org

Table of Contents

Executive Summary

This report aims to support stronger state-level efforts to combat ransomware, by showing existing connections between States and Threat Actors. Central to this effort is a dataset connecting ransomware threat actors to countries, drawing on judicial decisions, law enforcement operations, and both technical and political attributions. Because ransomware is a transnational crime, understanding these country connections requires a multilateral response that goes beyond what unilateral efforts for victim redress can achieve.

This report analyzes three standalone datasets, each answering a different question:

- To which countries are threat actors connected? A country–threat actor dataset (n=290).
- What can infrastructure research tell us? A sample of infrastructure data related to the activities of 24 threat actors (1,157 IPs; 312 netblocks; 60 countries).
- Who is being targeted and where? A global ransomware incidents record covering 2,753 incidents (2020–2025).

Most assessed country connections cluster in a few jurisdictions. Of the 290 threat actors, 42% lack sufficient data to assess a link. The remaining 168 connect to 40 countries. A large share are connected to the Russian Federation, followed by Iran and China. Connections are presented with varying degrees of confidence and do not imply state affiliation.

The infrastructure sample shows concentration and reuse. Several providers recur across different actors. Multiple overlap events appear, including exact IP reuse by different actors. These patterns indicate pressure points for disruption but are not used to assign connections between threat actors and countries.

The incidents dataset logs 2,753 cases from 2020 to 2025. It covers 21 sectors in 99 countries and attributes activity to 162 actors. The United States has the highest count, followed by the United Kingdom and Australia. Healthcare is the most targeted sector, followed by public administration and education. A large number of cases remain unattributed; the most attributed incidents involve *LockBit* and *ALPHV/BlackCat*.

Overall, the data shows persistent activity, shared infrastructure, and concentrated country connections. While this report offers a base for understanding these dynamics, its impact depends on the continuation of this research in collaboration with other stakeholders.

Ransomware: A Crime Beyond Accountability

Ransomware has emerged as a pervasive and destructive form of cyber extortion, with its impact now widely recognized across sectors. In 2024, industry analyses estimate compromised organizations pay an average of USD 1 million in ransom and incur around USD 1.5 million in recovery costs. However, the broader consequences for targets often far exceed the financial cost. Countries, especially those with low and middle incomes, are particularly vulnerable to the destructive force of ransomware. Prime examples include the *Conti* and *Hive* ransomware operations, which crippled Costa Rica's public administration, prompting a May 2022 state of emergency; and the September 2025 disruptions at several major European airports, which the EU's cybersecurity agency attributed to a third-party ransomware attack on automated check-in systems.

In response to this growing threat, a robust multistakeholder mobilization has taken shape, drawing on the expertise of academia, civil society, the private sector, and the research community. Prime examples include The Ransomware Task Force (RTF) providing a comprehensive framework for governments and industry to combat ransomware, and Virtual Routes' Pharos Series which presents a playbook for understanding ransomware operations and how to disrupt them. Malicious infrastructure mapping and takedown initiatives include the Shadowserver Foundation and Microsoft's Digital Crimes Unit cooperating with law enforcement to support botnet dismantling efforts, while the No More Ransom initiative supports ransomware targets in recovering their data without funding the criminals. Alongside many other initiatives, these efforts have made resilience gains possible.

> For a synthesis of effective public-private operations against cybercrime, see **World Economic Forum, *Disrupting Cybercrime Networks: A Collaboration Framework* (11 November 2024)**, which identifies collaboration **incentives, governance, and resourcing** as prerequisites for sustained disruption

Despite these efforts, the ransomware threat continues to escalate, with a 275% year-over-year increase in ransomware attacks according to Microsoft in 2024. Another report from Cyberint shows that the newly emerged ransomware threat actor *RansomHub* surpassed older brands with 531 leak-site posts in 2024, while also noting that half of the ten most active threat actors in Q4 2024 did not exist at the start of the year. The pace of increase is expected to continue, partially driven by newer technologies such as generative AI and the expansion of darknet cybercriminal markets - trends that continue to lower the knowledge barrier for engaging in criminal activities.

The national and international response to ransomware must maintain the pace at which the ransomware ecosystem evolves. While the 2023 takedown of *ALPHV/BlackCat* and the 2024 operation targeting *LockBit* disrupted specific operations of certain threat actors, law-enforcement actions had limited overall impact. Fundamentally, addressing ransomware comes down to state action, yet current national and international responses remain insufficient in delivering justice and redress for victims, and enforcing accountability for ransomware perpetrators.

This report aims to support stronger state-level efforts to close that gap.

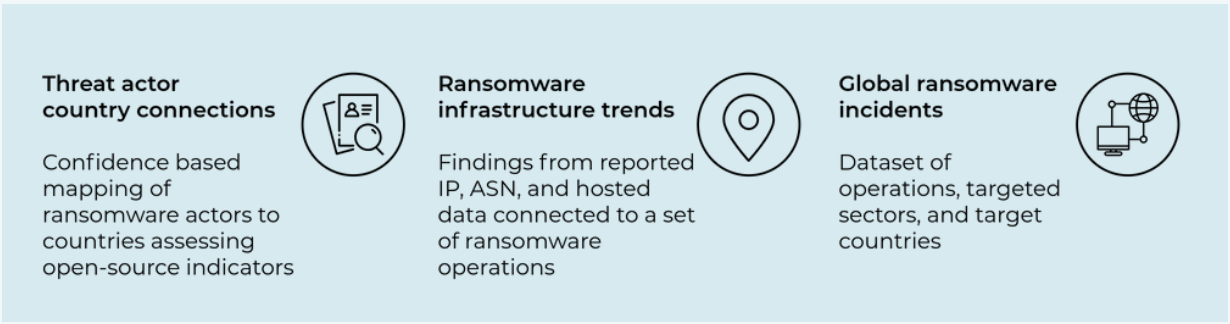
Advancing Accountability Through Data

Since 2020, the CyberPeace Institute has systematically analyzed cyberattacks, including ransomware and disseminated its findings via three publicly accessible platforms. Particular attention has been given to the targeting of civil society organizations, cyberattacks against the healthcare sector during the COVID-19 pandemic, and cyberattacks following the 2022 invasion of Ukraine.

This report builds on that foundation and expands its scope to encourage state action in enforcing accountability and securing justice for victims. Central to this effort is a dataset connecting ransomware threat actors to countries, drawing on judicial decisions, law enforcement operations, and both technical and political attributions. Because ransomware is a transnational crime, understanding these country connections requires a multilateral response that goes beyond what unilateral efforts for victim redress can achieve.

The report also examines a record of global ransomware incidents to identify targeting trends (2020-2025) and a sample of technical infrastructure data associated with 24 ransomware threat actors to reveal patterns of infrastructure use.

Figure 1. Mapping of datasets



Theory of Change

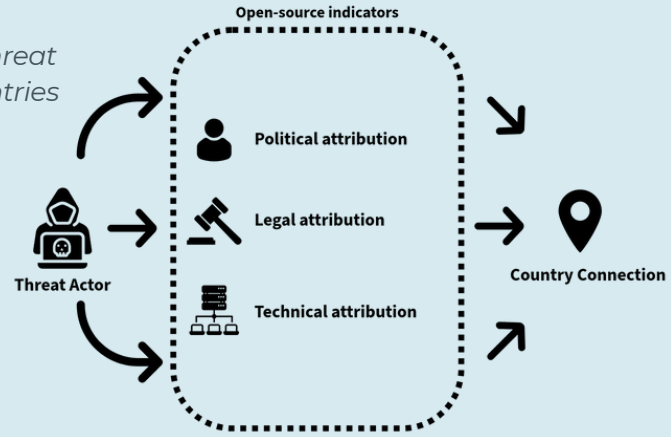
The underlying premise of this research is that curated information on jurisdictions leveraged by ransomware threat actors and host countries of malicious infrastructure can improve cross-border cooperation and discourage the persistence of safe havens for ransomware threat actors. By equipping states with actionable intelligence, this report aims to strengthen coordinated international responses and contribute to the global effort to hold ransomware threat actors accountable.

Mapping Country–Threat Actor Connections

This report assesses the connections between ransomware threat actors and countries based on open-source indicators. These indicators aim to expose operational and strategic links that can inform targeted disruption efforts. Assessments are categorized as High, Medium, and Low to express confidence levels in these connections. The assessed confidence is based not only on individual indicators but also cases where multiple indicators compound to inform the assessment.

The Institute does not conduct its own independent attribution efforts but instead compiles attributions made by external entities, such as cybersecurity firms, government agencies, and independent researchers. In this report, the indicators used to map connections are drawn from these attribution efforts, focusing on technical, political, and legal attribution.

Figure 2.
Connecting Threat Actors to Countries



Exposing these connections can help state authorities to prioritize their efforts on a national and international level. This includes the identification of the necessary partnerships for effective disruption. As new regulatory frameworks (e.g. the national implementations of the UN Cybercrime Convention[1]) are introduced, the development of this knowledge base will enable the community to track how the landscape evolves and assess the efficacy of policy response.

[1] *Entry into force requires signature and ratification through national processes.*

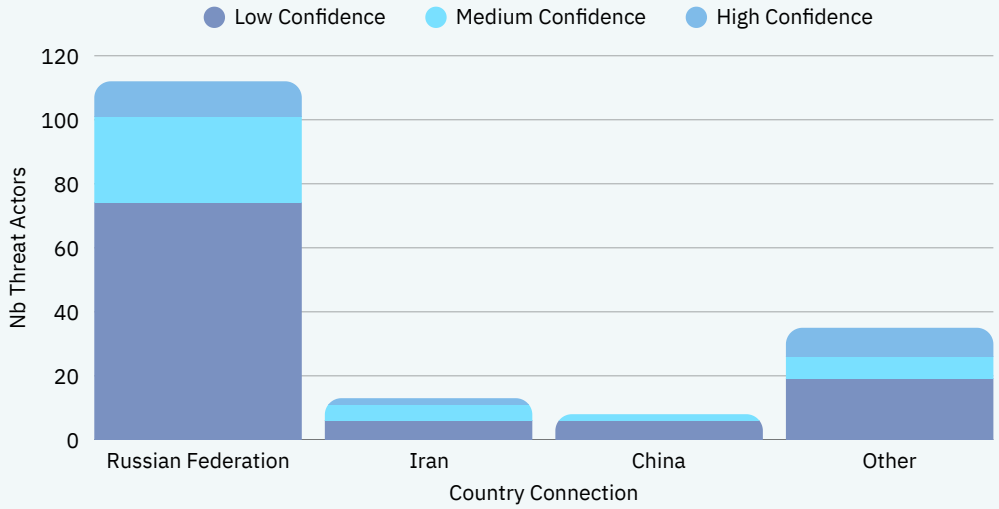
Key Findings

Key Finding 1
Threat Actor Country Connections

The analysis of threat actors' country connections reviewed 290 ransomware threat actors. Data is not available to assess the country connection of 122 threat actors (42% of 290). The remaining 168 threat actors are connected to 40 different countries,[2] with 67% (112 of 168) assessed, with a varying degree of confidence, to be connected to the Russian Federation, 8% (13 of 168) to Iran and 5% (8 of 168) to China.

Importantly, a connection to a country does not imply affiliation with that country's government or security services.

Figure 3. Country Connection Distribution of Threat Actors



- 22 are assessed with high confidence to be connected to at least one country, with 11 threat actors connected to the Russian Federation, followed by three to Ukraine and two to Iran.

- 41 are assessed with medium confidence to be connected to a country, with 27 threat actors connected to the Russian Federation, followed by five to Iran, and two to China, and Ukraine.

- 105 are assessed with low confidence to be connected to a country with 74 threat actors connected to the Russian Federation[3], six to China, and six to Iran.

[2] See Methodology for the definitions of connection country indicators
[3] This includes threat actors assessed with low confidence to be connected to the Commonwealth of Independent States (CIS); the CyberPeace Institute, however, classifies them as connected to Russia, the organization's most influential member state.

Key Findings

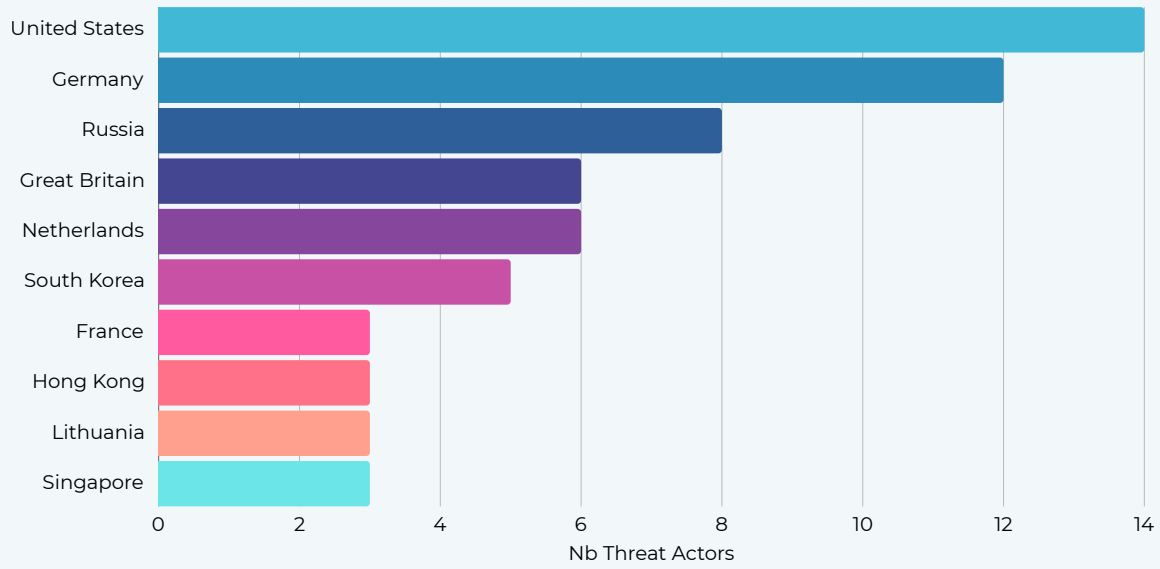
Key Finding 2
Ransomware Infrastructure Trends

The CyberPeace Institute analyzed technical infrastructure data reported for alleged use by 24 threat actors, collected from 17 different sources. The purpose of this analysis was to understand trends in the infrastructure use of a defined sample of threat actors.

While insufficient to base an assessment of country connections of threat actors, these findings provide information on the trends in the use of IP addresses connected to organizations that own autonomous system numbers (ASNs) connected to ransomware operations.

The 24 threat actors leveraged infrastructure tied to 1,157 IP addresses across 312 netblocks, with the IP addresses located in 60 countries. To understand where infrastructure is most frequently exploited, the analysis counted each threat actor once per country, regardless of how many IP addresses they used. This shows a concentration in a few jurisdictions, particularly the United States, Germany, and the Russian Federation.

Figure 4. Unique ransomware threat actors by country of IP address location



Findings also indicate that certain providers are highly likely to be favored by ransomware threat actors. Infrastructure from one provider was used by six of the 24 threat actors, while the next two were each used by five threat actors. All three providers are headquartered in the United States.

Key Findings

Key Finding 3

Global Ransomware Incidents (2020-2025)

The analysis of global ransomware activity covers a sample of 2,753 ransomware incidents (2020-2025) conducted by 162 threat actors against organizations in 21 sectors located in 99 countries. Organizations in the United States (1488), United Kingdom (175) and Australia (141) were targeted the most.

Figure 5. Top Five Most Targeted Countries

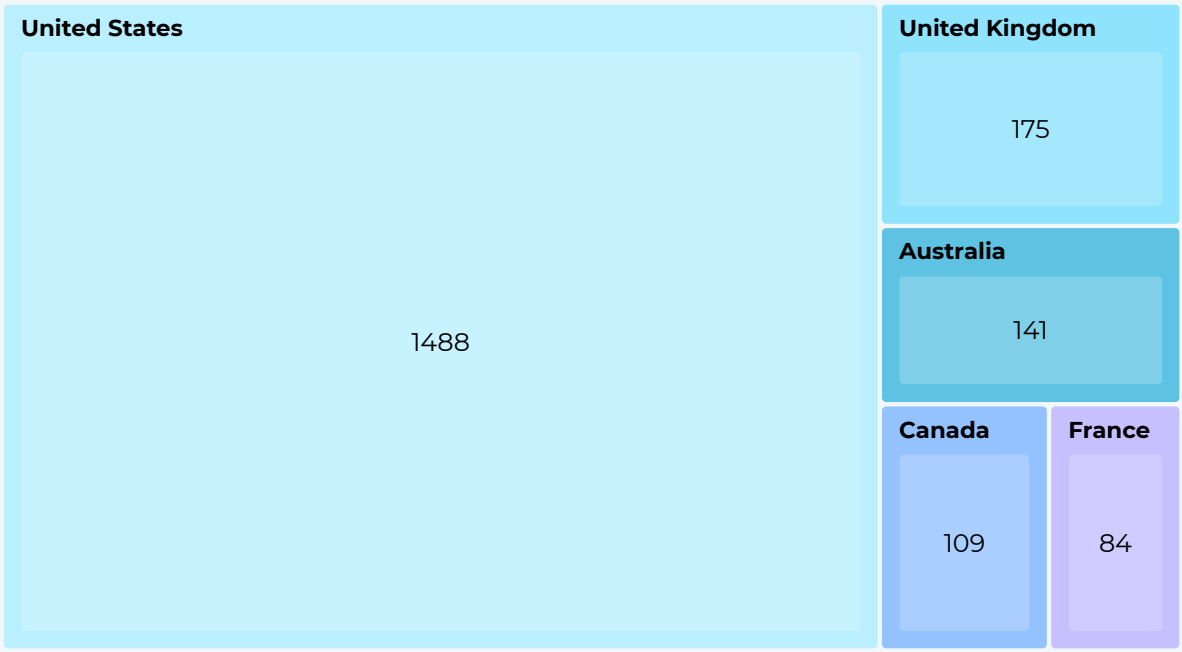


Figure 6. Top Five Most Targeted Sectors

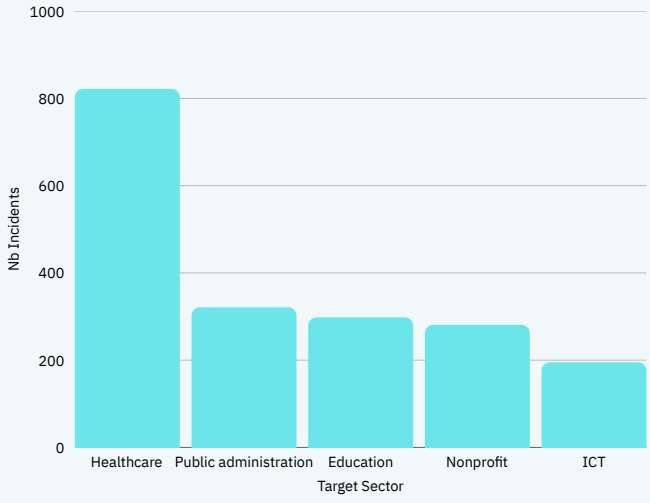
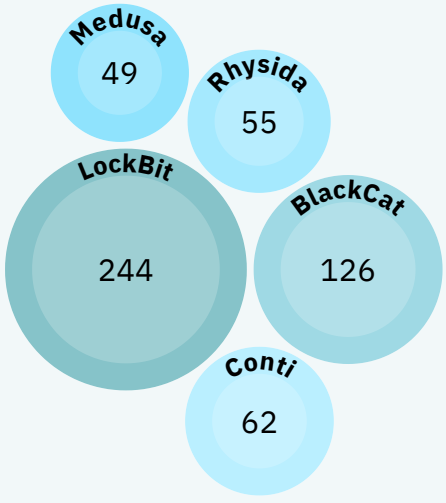


Figure 7. Top Five Threat Actors



Key Terms

Attribution: The act of identifying a threat actor responsible for a cyber operation. The CyberPeace Institute does not conduct its own attribution but instead draws on existing technical, political, and legal attributions made by external entities (e.g., cybersecurity firms, government agencies, independent researchers). The information and justifications underlying these attributions are used as open-source indicators to inform our confidence assessments of threat actor country connections.

- **Technical attribution:** Third-party efforts (state and non-state entities) to determine responsibility for a cyber operation based on the analysis of technical artifacts (e.g. through forensics analysis). Indicators include associating the attack to specific software (e.g. malware strain), hardware (e.g. a server), code or modus operandi (operational & behavioral indicators).

- **Legal attribution:** Decisions of the Judiciary that determine legal responsibility of a cyber operation. Indicators include named persons and geographic locations in judicial decisions.

- **Political attribution:** Public identification and assignment of responsibility for a cyber operation to specific threat actors by state officials. This may be informed by technical, legal and intelligence assessments but does not require states to disclose or substantiate underlying evidence. This form of attribution is expressed through official statements, sanctions, or diplomatic measures. Indicators may include named persons, threat actors, and geographic locations.

Bulletproof Hosting: defined by Europol as "a service offered by some sites or web hosting firms that allows their customers considerable leniency on the content they can upload. Such hosting providers tend not to respond to lawful requests for information".

Country Connection: The assessed connection between a threat actor and a country.

These connections are assessed through analysis of open-source indicators. Importantly, a connection to a country does not imply affiliation with that country's government or security services.

In this report, the CyberPeace Institute uses three categories for assessing confidence levels:

- **High confidence** - highest degree of assessed confidence in threat actors' country connection. This assessment is based on judicial decisions naming persons, law enforcement publications of operations against threat actors, or political attributions.

- **Medium confidence** - medium degree of assessed confidence in threat actors' country connection. This assessment is based on compounding evidence, collected from third party attribution efforts, such as, but not limited to, technical malware and infrastructure analysis, modus operandi, patterns in targeting.

- **Low confidence** - lowest degree of assessed confidence in threat actors' country connection. This assessment is based on limited amounts of evidence, such as operational and behavioral indicators alone. Operational and behavioral indicators are inferred from linguistic, cultural, and behavioral signals. Examples include the language used in ransom notes or leak sites, patterns of forum activity, and targeting behaviors that suggest a geographical or cultural affiliation. Linguistic markers, however, might be deceptive due to false-flagging and copy-paste reuse and are therefore used as weak indicators unless corroborated. Threat actor self-attribution to a country is assessed as low confidence, unless corroborated by other sources.

Cyber Operation - A commonly used term to describe actions by a nation state or state sponsored or affiliated group to penetrate a target's computer or networks through the use of offensive cyber capabilities such as hacking, malware or other methods with the intention to damage, deny, disrupt, degrade, destroy, surveil, or manipulate targets to achieve political, military and/or strategic goals. Cyber operations are a means or method of warfare when used in a situation of armed conflict.

Digital Public Infrastructure - defined by World Economic Forum as "the essential digital systems and platforms that enable individuals, businesses and communities to participate in the digital economy and society. These systems function as core frameworks to facilitate reliable, safe equitable access to digital goods and services, and empower stakeholders to build value through scaled digital capacities.

Digital public infrastructure (DPI) is built on physical infrastructure, like data centres and communications networks, and includes foundational elements like digital ID protocols and data exchange platforms and extends up to digital interfaces engaged directly by users."

Malicious Infrastructure: defined by Flare as "the underlying hardware, software, or networks used by attackers to carry out cyberattacks or illegal activities."

Ransomware: Ransomware is a type of malware used to encrypt a target's data and/or systems, extorting a ransom in exchange for a decryption key.

Threat actor: Also known as cyber threat actors or malicious actors, these are individuals or groups that intentionally cause harm to digital devices, networks, or systems. Threat actors are any group of individuals or individuals responsible for the development, deployment, and/or facilitation of ransomware attacks.

Words of Estimative Probability (WEPs): terms used by intelligence analysts to qualitatively assess the likelihood of specific statements. The CyberPeace Institute uses the PHIA probability yardstick. See methodology for further details.

Analysis

This report examines the country connection of ransomware threat actors. Assessments are expressed with three categories of confidence: *High*, *Medium*, and *Low*.

These connections are assessed through analysis of open-source indicators. Importantly, a connection to a country does not imply affiliation with that country's government or security services.

While ransomware constitutes a transnational threat, the main body of this analysis will focus on the findings of country connection research, specifically examining the primary country connection associated with each identified threat actor. Following this, a separate section presents a subset of threat actors assessed to be connected to more than one country.

Secondly, the report highlights trends in the global landscape of ransomware operations and the threat actors involved, with a focus on targeted sectors and countries.

Lastly, while insufficient to connect threat actors to specific countries, the findings of the infrastructure data analysis provide information on the geographic locations of organizations that facilitate ransomware operations through their services.

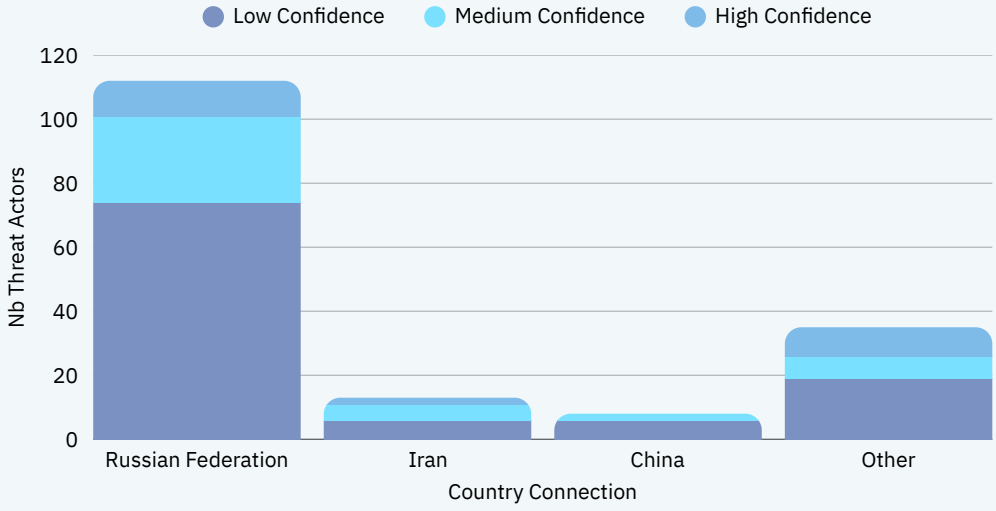
Threat Actor Country Connections

The CyberPeace Institute collected, collated, and analyzed data on 290 ransomware threat actors. The dataset spans threat actors regardless of activity time periods to capture broad patterns in threat actor country connections.

Figure 8. Country Connection Distribution of Threat Actors

Data is not available to assess the country connection of 42% of all studied threat actors. The remaining 168 threat actors are connected to 40 different countries,[4] with 67% (112 of 168) assessed, with a varying degree of confidence, to be connected to the Russian Federation, 8% (13 of 168) to Iran and 5% (8 of 168) to China.[5] Percentages in this section are calculated out of the 168 threat actors with assessed country connections.

Figure 9. Country Connection Distribution of Threat Actors



[4] See Key Terms for the definition used for 'country connection'.
[5] Indicators used to map connections are detailed in the Key Terms.

High Confidence Connections

We assess with high confidence that 22 ransomware threat actors are connected to at least one country, with 11 threat actors connected to the Russian Federation, followed by three to Ukraine, and two to Iran.

To illustrate our country connection assessment, we use *Evil Corp* as an example. *Evil Corp* is a ransomware threat actor assessed with high confidence to be connected to the Russian Federation. This assessment is based on a coordinated law enforcement operation that resulted in indictments and sanctions in December 2019, led by the UK National Crime Agency in partnership with the governments of the United States, United Kingdom, and Australia.

The disruption of *Evil Corp* led to the fragmentation of its original personnel, resulting in splinter threat actors, such as *Phoenix*, *Macaw,* and *DoppelPaymer*. Assessed to be connected to both *Evil Corp* and the Russian Federation with a high degree of confidence, the CyberPeace Institute categorizes them as separate and distinct threat actors, as the organizational structure of the original actor had changed.

Another example is *Cl0p*, a threat actor assessed with medium confidence to be connected to Ukraine based on an INTERPOL-coordinated law enforcement operation, Operation Cyclone. This operation targeted 21 locations in Kyiv, resulting in the arrests of six *Cl0p* members and the seizure of servers and luxury cars in 2021. INTERPOL noted that the six suspects were "tightly linked to a Russian-language cybercriminal gang" responsible for approximately $500 million in ransomware proceeds. This indicates operational activity in Ukraine and a connection to a Russian-language criminal network.

An example for a high confidence country connection assessment to Iran is *SamSam*. This is based on a grand jury indictment in Newark, New Jersey, against two individuals responsible for its operations.

Medium Confidence Connections

There are 41 threat actors assessed with medium confidence to be connected to a country, with 27 connected to the Russian Federation, followed by five to Iran, two to Ukraine and two to China.

A medium confidence is based on compounding open-source indicators, such as third-party attribution efforts and law enforcement operations resulting in arrests, but without a definitive judicial decision. For example, *Bronze Starlight* is assessed with medium confidence to be connected to China, based on compounding evidence from third-party technical attribution analyses.

Low Confidence Connections

Finally, data is available on 105 threat actors assessed with low confidence to be connected to a country, with 74 connected to the Russian Federation[6], six to Iran, and six to China.

A low confidence country connection is assessed when there is limited evidence, primarily based on operational and behavioral indicators. For example, *FIN10* is assessed with low confidence to be connected to Canada. All of the known compromised organizations were Canadian, concentrated in the mining, natural resources, and casino sectors - an exclusive regional focus that suggests localized knowledge and intent rather than indiscriminate targeting. FireEye observed that *FIN10*'s operational activity, including file creation timestamps and C2 communications, aligned with North American Eastern Time business hours (observed timestamps). Some of the threat actor's infrastructure was geolocated to Canadian hosting providers, and victim communications showed linguistic fluency consistent with North American English. While these indicators are not conclusive on their own, we assess with low confidence that *FIN10* is connected to Canada.

Another example is *RTM Locker* - assessed with low confidence to be connected to the Russian Federation. This assessment is based on web posts written both in English and Russian language, with higher quality content in Russian, supporting the indication of the latter as the threat actor's native language. Additionally, the threat actor avoids targeting within the CIS region.

As a last example, ransomware threat actor *D0Glun* is assessed with low confidence to be connected to China due to its use of Chinese language in its ransom instructions.

Transnational nature of ransomware

While the analysis of assessed connection countries of threat actors focused on the primary country, in reality, many ransomware threat actors are connected to more than one. Our data suggests that at least 30 threat actors have been connected to more than one country, and 13 to more than two countries. For example, *NetWalker* is a ransomware threat actor, whose developer is assessed with low confidence to be based in the Russian Federation, and whose operations spanned across several jurisdictions - affiliates to the ransomware have been arrested in Canada and Romania, while Bulgarian authorities took down a server used by the ransomware, and Polish authorities arrested five

[6] This includes threat actors assessed with low confidence to be connected to the Commonwealth of Independent States (CIS); the CyberPeace Institute, however, classifies them as connected to Russia, the organization's most influential member state.

people in relation to the operations of a bulletproof hosting service that facilitated *NetWalker*'s operations. Personnel from *DoppelPaymer* were arrested in Germany, and Ukraine, while the other personnel are of Russian origin, with the alleged leader reportedly living in the Russian Federation, according to the Federal Criminal Police Office of Germany. Another example is *LockBit* - one of the most active ransomware threat actors, whose members, mostly Russian citizens, were arrested in Israel, France, United Kingdom, Canada. In Spain, law enforcement authorities arrested the administrator of a bulletproof hosting service facilitating *LockBit* operation.

Global Ransomware Incidents

The analysis has been conducted on a sample of 2,753 ransomware incidents that occurred between 2020 and 2025. The incidents were conducted by 162 threat actors[7], targeting organizations in 21 sectors across 99 countries.

Figure 10. Target Country Distribution (2020-2025)

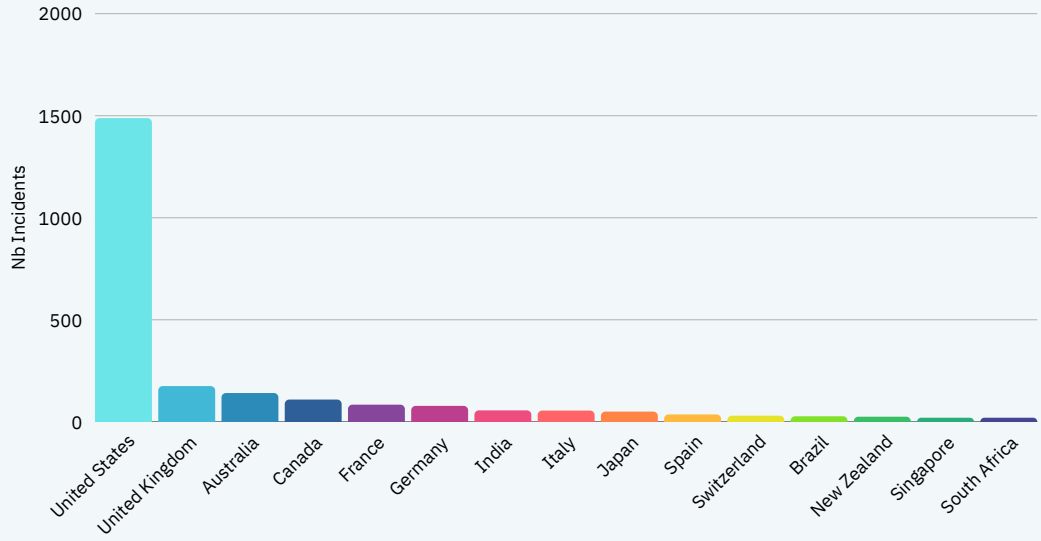
Out of the ransomware incidents registered, a significant number of cases (1142) remain unattributed to a specific threat actor. The most ransomware attacks have been attributed to *LockBit* (244), followed by *ALPHV/BlackCat* (126), *Conti* (62), *Rhysida* (55), and *Medusa* (49). The top five threat actors together account for 536 incidents (19.5%) of the 2,753 sample.

Geographically, the highest number of ransomware incidents have been recorded against organizations in the United States (1488), representing 54% of all incidents recorded during the study period. The United Kingdom and Australia follow, with 175 and 141 incidents respectively.

The sample of open-source collected ransomware incidents aligns with other research, which shows that the United States accounts for roughly half of all global ransomware incidents that occurred in 2024, with reports placing its share between 46% and 50% of attacks. This disproportionate targeting stems from several factors: U.S. organizations operate some of the world's largest and most profitable industries, such as manufacturing, healthcare, energy, and technology, offering threat actors both valuable data and the financial capacity to pay substantial ransoms.

[7] Only 162 of the 290 researched threat actors appear in our Global Ransomware Incidents (2020-2025) dataset. This discrepancy is due to factors such as limited availability of corroborated open-source information, disrupted operations, rebranding, inactivity and other causes.

Figure 10. Target Country Distribution (2020-2025)

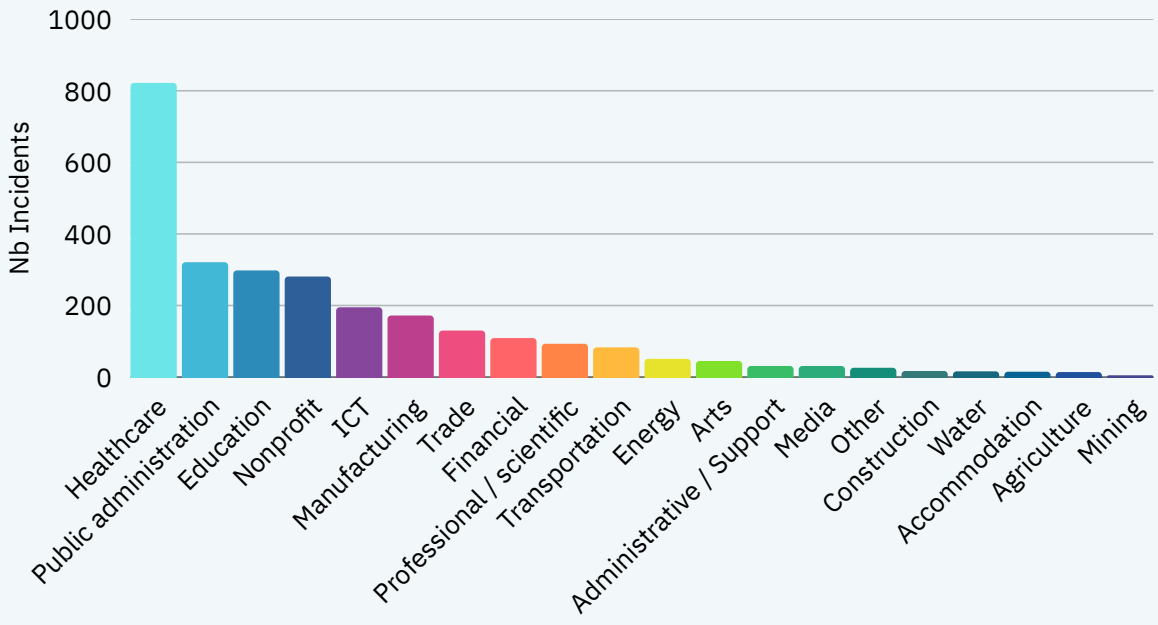


Geopolitical dynamics amplify this trend, as more than 80% of the ransomware threat actors analyzed in this report are assessed, with varying degrees of confidence, to be connected to countries often considered geopolitically adversarial to the United States. In addition, Chainalysis estimates global ransomware payments exceeded USD $1.1B in 2023, reinforcing the profitability of these campaigns.

Targeted Sectors

The data identifies healthcare as the most targeted sector, with 818 recorded incidents, followed by public administration (318) and education (298).

Figure 12. Target Sector Distribution (2020 - 2025)



Healthcare Focus

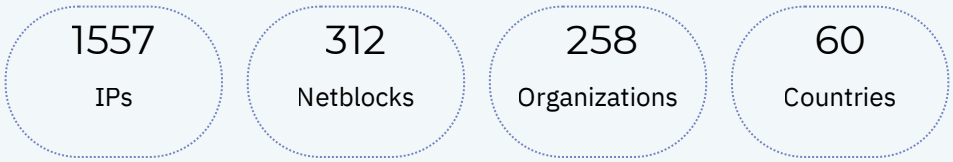
According to the U.S. Department of Health and Human Services in 2024, *"Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware."*. This is likely driven by several factors. In the United States, mandatory reporting requirements under federal and state laws, including HIPAA regulations, lead to greater public disclosure of incidents compared with other sectors. Attacks on hospitals and healthcare providers tend to be highly visible, often disrupting critical services and generating significant media coverage. The sector also processes and stores large volumes of sensitive personal and medical data, making it attractive to ransomware operators. Additionally, healthcare organizations often operate in complex technology environments that integrate legacy systems, electronic health records, medical devices, and third-party services, all of which can expand the attack surface and facilitate lateral movement. Combined with resource and staffing constraints, these factors make the sector a consistently high-value target for opportunistic ransomware threat actors. Additionally, as ransomware attacks against the healthcare sector can pose an immediate threat to patient wellbeing, healthcare organizations are more likely to pay ransoms to restore services quickly.

Ransomware Infrastructure Trends

Along with researching the connections to countries of ransomware threat actors, the CyberPeace Institute also analyzed infrastructure data related to 24 threat actors collected from 17 different sources.[8]

While insufficient to base an assessment of country connections of threat actors to specific countries, the findings of the infrastructure data analysis provide information on the geographic locations of organizations that facilitate ransomware operations through their services. While not exhaustive, the aim is to demonstrate an approach for identifying patterns in hosting provider reliance and shared infrastructure. Expansion of this dataset to cover additional threat actors, infrastructure, and longer timeframes would strengthen collective efforts.

The infrastructure research relied on a dataset of reported alleged infrastructure usage between Q1 2023 and Q1 2025. Findings indicate that these 24 threat actors leveraged infrastructure tied to 1,157 IPs[9] across 312 netblocks[10], owned by 258 organizations that own the ASN[11] routing these IP addresses located in 60 countries, to conduct or facilitate their ransomware operation.[12]



To understand where infrastructure is most frequently exploited, the analysis counted each threat actor once per country, regardless of how many IP addresses they used. This shows a concentration in a few jurisdictions, particularly the United States, Germany, and the Russian Federation, as shown in Figure 4 (Key Findings).

Based on reported activity associated with this infrastructure, threat actors employed it primarily for command-and-control (C2)[13] purposes, with occasional use for malware payload delivery.

---

[8] ThreatFox; VirusTotal ; Censys ; CISA Cybersecurity Advisories ; Canadian Centre for Cyber Security ; Cybereason ; Palo Alto Networks Unit 42 ; Qualys Blog ; Sygnia ; Trend Micro ; Cisco Talos Intelligence Blog ; Redacted ; Darktrace Blog ; ReliaQuest Blog ; Infoblox Blogs ; ReversingLabs Blog ; NCC Group Blog

[9] A unique identifier assigned to a device on the internet or a local network.

[10] Refers to "a range of IP addresses that are grouped together under a specific address space" `The owner of a netblock can be found by using tools such as IPInfo.io.

[11] Defined by Cloudflare as "a large network or group of networks that has a unified routing policy. Every computer or device that connects to the Internet is connected to an AS."

[12] While this can indicate preferences for infrastructure hosting and locations it should not be used to attribute actual physical location to threat actors since the availability of digital services for web hosting for example means actors can use third party services based in various countries and unrelated to their actual physical locations.

[13] The technical infrastructure established by a threat actor to manage compromised systems.

Central to the infrastructure analysis was identifying each IP address's associated autonomous system number (ASN), the organization that owns the ASN routing these IP addresses, and its hosting location at the time of the activity (where verifiable)[14]. This enabled the team to correlate usage across actors and determine overlaps in the digital resources they exploited.

The following observations were made:

- **Shared hosting providers:** Various threat actors relied on the same service providers for hosting or related services.
- **Proximity and reuse of IP addresses:** Correlation of reported IPs showed instances where the same address was used[15] by more than one threat actor within a short period, and cases where multiple actors operated within a small set of IPs on the same network.

These findings indicate that threat actors are highly likely to favor certain providers. Infrastructure from one provider was used by six of the 24 threat actors, while the next two providers were each used by five threat actors. The headquarters of the top three most used providers are registered in the United States.

Factors highly likely influencing this preference include ease of access, competitive hosting costs, and, potentially, less-rigorous abuse-monitoring and takedown practices.

Finally, the data revealed six instances of infrastructure overlap events involving multiple threat actors. In five cases, the exact same IP address was reused across threat actors (sometimes within short timeframes), while one case involved different IPs within the same hosting network, suggesting likely links or shared infrastructure between threat actors. Please see Table 1.

[14] ASN ownership and geolocation were resolved to the point-in-time of malicious use.
[15] While shared or adjacent IPs can occur due to shared hosting, this is less likely here because the top IP owners in our dataset control thousands of addresses, reducing the chance of overlap by coincidence.

Table 1. Reuse of IP addresses by multiple ransomware threat actors

IP Address	Threat Actor(s) Observed	Function	First Seen (Threat Actor A)	First Seen (Threat Actor B)	Overlap Type
108[.]181[.]115[.]171	*RansomHub* → *BianLian*	C2	1/16/2025	3/22/2025	Exact IP Reuse (Sequential)
162[.]33[.]179[.]114	*Medusa* → *ALPHV/BlackCat*	C2	6/30/2023	7/25/2023	Exact IP Reuse
162[.]33[.]179[.]116	*BianLian* → (Network shared w/ *Medusa & ALPHV)*	C2	10/5/2023	11/22/2023	IP on Same Network
95[.]179[.]189[.]177	*BianLian* → *BlackBasta*	Go Trojan C2 (BianLian), Cobalt Strike domain C2 (BlackBasta)	6/3/2024	3/14/2024	Exact IP Reuse
176[.]105[.]202[.]212	*BianLian* → *ALPHV/BlackCat*	Go Trojan C2 (BianLian), Payload Delivery (ALPHV/Black Cat)	1/2/2023	12/3/2024	Exact IP Reuse (Long Gap)
134[.]195[.]88[.]27	*BianLian* → *Medusa*	Go Trojan C2 (BianLian), C2 (Medusa)	4/28/2023	12/11/2023	Exact IP Reuse

Ransomware in International Discussions

The findings of this report have direct implications for the implementation of States' commitments under the UN Framework for Responsible State Behavior in Cyberspace and the United Nations Cybercrime Convention (UNCC). By identifying where ransomware threat actors are connected to countries, how they use infrastructure, and who they target, the report provides insights to help States enforce their obligations and strengthen accountability.

Key insights include:

- **Concentration of threat actors in a few jurisdictions:** This underscores the importance of targeted diplomatic engagement and operational cooperation to disrupt criminal use of national territories and to reinforce due diligence obligations (Norm c; UNCC arts. 21–22, 35–46).

- **Shared infrastructure across threat actors:** Multiple ransomware threat actors rely on overlapping hosting and network services, creating exploitable points of failure. Coordinated cross-border action can significantly reduce these vulnerabilities (Norm d, h; UNCC arts. 22, 35–46).

- **Targeting of healthcare systems:** Persistent ransomware attacks against healthcare undermine critical infrastructure protection and highlight urgent needs for resilience and international support (Norm g; UNCC arts. 34–35, 54).

Addressing ransomware therefore supports both binding and non-binding obligations: from preventing malicious cyber activity and strengthening critical infrastructure to ensuring cross-border cooperation and victim protection. These findings can guide States in operationalizing norms and treaty provisions.

The CyberPeace Institute will continue this research by monitoring and assessing how States implement these measures, ensuring accountability is pursued in collaboration with the multi-stakeholder community.

Closing Remarks

This report aims to demonstrate both the scale and persistence of the ransomware ecosystem and the value of systematically connecting threat actors to countries and identifying trends in shared infrastructure, and targeted sectors and countries. While this report offers a base for understanding these dynamics, its impact depends on the continuation of this research in collaboration with other stakeholders, including policymakers, law enforcement, technical experts, and civil society to enrich datasets, refine attribution methodologies, and expand the scope of analysis.

Future collaboration should not be limited to information-sharing but could potentially also include capacity-building initiatives for the most affected and vulnerable sectors, such as healthcare and nonprofits. Such partnerships can create a continuous feedback loop, where operational lessons may inform policymaking, and in turn enable more effective disruption of ransomware operations.

Insights from this report and from future collaborative work should feed directly into domestic and multilateral legal and policy processes, including the UN's responsible state behavior framework and the UN Cybercrime Convention. By linking technical findings to legal obligations states can:

- Close jurisdictional gaps through targeted diplomatic and operational cooperation.
- Target shared infrastructure as pressure points against threat actors.
- Protect critical infrastructure sectors through minimum security baselines, resilience funding, and coordinated international support.

By sustaining and expanding this research in collaboration with others, the CyberPeace Institute and its partners can help ensure that ransomware operations are not only monitored and documented, but are also addressed with a coherent, collective, and legally grounded response.

Methodology

This report does not claim to present an exhaustive or comprehensive account of ransomware threat actors and related activity since the first documented cases in the late 1980s (e.g., the 'AIDS Trojan' of 1989). Instead, it identifies trends and patterns in global ransomware incidents between 2020 and 2025, while examining threat actors across a broader period where sources are available, with particular attention to the countries to which those actors are assessed to be connected.

Research Approach

The primary method was desk-based research conducted in English, French, Spanish, Italian, Russian, Ukrainian, and Bulgarian. The main categories of data sources included (but were not limited to):

- Cybersecurity firm reports and threat intelligence databases;
- Official governmental and law enforcement publications;
- Industry and academic studies;
- News media and other publicly available open-source repositories.

Threat Actor Research

The ransomware threat actor dataset relied on external attribution efforts. The Institute deliberately avoided engaging in debates around rebranding or renaming of threat actors. The dataset includes ransomware threat actors active across all time periods, without a fixed temporal scope, to ensure a broad understanding of patterns in threat actor–country connections beyond the constraints of specific timeframes.

This approach enables the aggregation of expert assessments, but introduces potential biases and inconsistencies, since attribution methodologies vary and may be shaped by geopolitical, economic, or institutional perspectives (Rid & Buchanan, 2015). Reliance on external sources also means that disputed or erroneous attributions may enter the dataset, affecting accuracy.

To mitigate these risks, every threat actor included in the dataset had to be:

- Identified as a unique ransomware threat actor, and
- Profiled by at least two distinct external sources as such.

Global Ransomware Incident Dataset - Inclusion Criteria

The inclusion criteria for the global ransomware incident database required collecting available data on ransomware incidents (2020-2025) reported by sources with established reputations. Incidents reported solely by ransomware threat actors, without corroboration from independent or reputable sources, were excluded.

Because this dataset incorporates material collected for earlier CyberPeace Institute projects - Cyber Incident Tracer #Health (exclusively traced cyberattacks against the healthcare sector), Cyber Attacks in Times of Conflict #Ukraine, and CyberPeace Tracer (exclusively traces cyberattacks against nonprofits) - results of the global ransomware analysis may be skewed toward healthcare, nonprofit, and conflict-related targets. This constitutes a sampling bias common to sector-focused research.

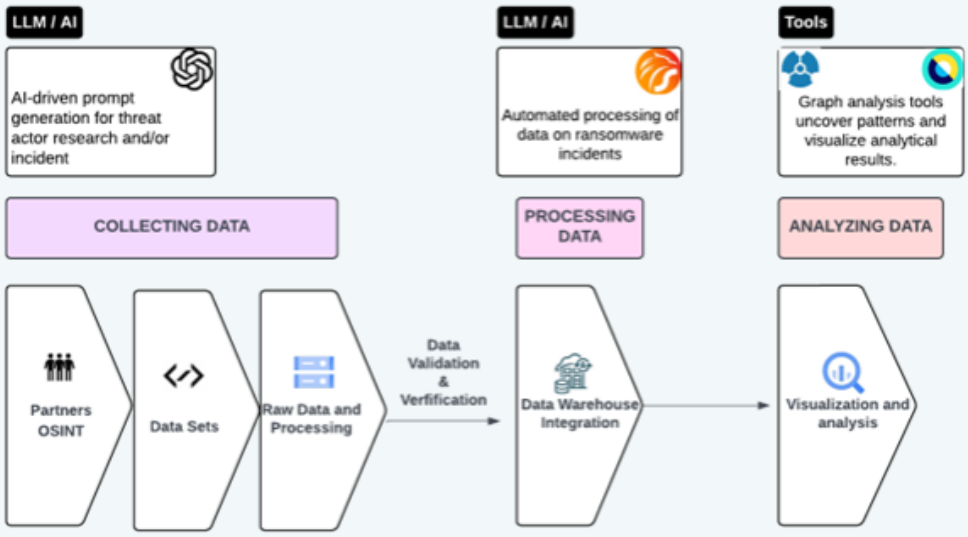
Data Processing and Analysis

All collected, collated, and analyzed data was stored in the CyberPeace Institute's secure data warehouse.

- For ransomware threat actors: GPT – 4o was leveraged primarily for data discovery, while entity extraction and validation relied more heavily on manual review.

- For ransomware incidents (2020–2025): data was extracted using a platform that extended ChatGPT 3.0 capabilities to process and analyze lists of URLs, automating part of the extraction workflow. Thereafter, an analyst manually validated and verified all extracted information, ensuring reliability.

Figure 13. CyberPeace Institute's Data Pipeline



For Ransomware Infrastructure Trends:

- The ThreatFox dataset was first exported and filtered by reported year to align with the reporting timeframe. The data was then narrowed to include only domains, IP addresses, ports, and URLs associated with all available ransomware threat actors in the aforementioned source.

The original ThreatFox export did not contain information on ASN ownership, company names, or hosted locations for associated IP addresses at the time of reporting. To enrich the dataset with this information:

- We first reviewed researcher comments on the ThreatFox interface that mentioned ASNs, companies, or IP locations at the time of reporting.

- When unavailable or to cross-check, we consulted ipinfo.io and similar tools to obtain the current IP location, then verified against VirusTotal and other sources for historical records. Researcher contributions in VirusTotal were particularly useful for identifying previous ASN assignments or locations.

- BGP.tools / BGP View and historical WHOIS records (e.g., org-name entries available via VirusTotal) were used to determine IP ownership and full organizational names at the time an IOC was reported. This was essential because in several cases, ownership or geolocation of IP space had changed in the years since the IOC was originally logged.

For domains, we mapped them to IP addresses using historical DNS records (available in VirusTotal and other platforms), then applied the same enrichment process to establish IP ownership at the relevant point in time.

To expand coverage, we reviewed multiple third-party reports and publications to extract time-specific IOCs. The same methodology was applied to these datasets, ensuring consistent attribution of hosting providers, ASN ownership, and geolocation.

Finally, by ensuring that all domains had associated point-in-time IP mappings, we enabled correlation across datasets highlighting instances where different domains shared common infrastructure (IP addresses or providers) at the time they were reported as malicious.

Challenges and Limitations

Open-source intelligence (OSINT) is inherently constrained by the availability, accessibility, and reliability of publicly disclosed information. Many cyber incidents remain unreported, particularly when organizations lack the capacity or incentive to disclose attacks. Furthermore, analysts may encounter difficulties in identifying and integrating emerging data sources, leading to potential gaps in the dataset. The complexity of cyberattack reporting, which varies in terminology, technical detail, and consistency across sources, further complicates data collection and standardization. Additionally, the absence of key variables, such as detailed attack vectors, motivations, and impact assessments, limits the depth of analysis that can be conducted.

The quality of the dataset is contingent on the verification process, which is subject to both time constraints and resource limitations. The need to cross-reference multiple sources to validate incidents and their details may result in delays in data inclusion. Furthermore, as cyber threats evolve rapidly, there is a risk that the dataset does not capture the latest attack techniques or emerging threat actors in real-time.

Attributing ransomware threat actors to specific countries using open-source indicators faces significant limitations. Law enforcement and judicial sources disclose only partial evidence due to legal constraints, while third-party attributions vary in methods and may be influenced by commercial or political interests. Open data is vulnerable to misinformation and deliberate obfuscation, as threat actors reuse infrastructure, adopt "Ransomware-as-a-Service" models, and plant false linguistic or behavioral cues. Additionally, groups frequently rebrand or fragment, potentially causing inconsistencies in data collection and assessment, which further complicate analysis; however, absence of attribution cannot be equated with absence of activity. Geopolitical sensitivities, jurisdictional barriers, and the risk of politicization further constrain research.

When conducting analysis it is instrumental to accurately communicate probability in the assessment of our findings and inferences. The CyberPeace Institute uses the UK's Defence Intelligence standard for conveying probability; the 'Professional Head of Intelligence Assessment (PHIA) probability yardstick'.

This scale demonstrates broad ranges of certainty or uncertainty that can be translated into consistent language; this language is used throughout this report.

Figure 14. PHIA Probability Yardstick

Bibliography

·2025 Ransomware Report: Sophos State of Ransomware. Sophos, https://www.sophos.com/en-us/content/state-of-ransomware.

·AbuseIPDB - IP Address Abuse Reports - Making the Internet Safer, One IP at a Time. AbuseIPDB, https://www.abuseipdb.com/

·ALPHV/BlackCat Ransomware Targeting of Canadian Industries. Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/alerts-advisories/alphvblackcat-ransomware-targeting-canadian-industries.

·Aon's 2025 Global Cyber Risk Report Reveals Reputation Risk Events Can Reduce Shareholder Value by 27 percent. (n.d.). Aon Plc Global Media Relations. Retrieved August 18, 2025, from https://aon.mediaroom.com/2025-06-17-Aons-2025-Global-Cyber-Risk-Report-Reveals-Reputation-Risk-Events-Can-Reduce-Shareholder-Value-by-27-percent.

·BGP Toolkit and BGP ASN Routing Lookup Tool. BGP View, https://bgpview.io/.
·BGP Tools. BGP, https://bgp.tools/.

·BKA. "BKA - Fahndung Nach Personen - Facts of the Case." https://www.bka.de/DE/IhreSicherheit/Fahndungen/Personen/BekanntePersonen/Cybercrime_NRW/IOT/SV_englisch.html.

·Bleih, Adi. "Ransomware Annual Report 2024." Cyberint, 13 Jan. 2025, https://cyberint.com/blog/research/ransomware-annual-report-2024/.

·Burt, Tom. "New Action to Combat Ransomware Ahead of U.S. Elections." Microsoft On the Issues (blog), 12 Oct. 2020. https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/.

·Canada, Communications Security Establishment. Canadian Centre for Cyber Security, 15 Aug. 2018, https://www.cyber.gc.ca/.

·Canada, Communications Security Establishment. "ALPHV/BlackCat Ransomware Targeting of Canadian Industries." Canadian Centre for Cyber Security, 25 July 2023, https://www.cyber.gc.ca/en/alerts-advisories/alphvblackcat-ransomware-targeting-canadian-industries.

·Censys, https://censys.com/

·Chiappetta, Tony. “Why US Businesses Are the Top Ransomware Target in 2025.” https://prevent-ransomware.com/blog/why-us-businesses-are-the-top-ransomware-target-in-2025

·Cisco Cyber Threat Trends Report. Cisco Umbrella, https://umbrella.cisco.com/info/cyber-threat-trends-report.

·Cisco Talos Blog. Cisco Talos Blog, https://blog.talosintelligence.com/.

·Cloudflare. “What Is an Autonomous System? | What Are ASNs?”. https://www.cloudflare.com/learning/network-layer/what-is-an-autonomous-system/.

·Cloudflare. “What Is Routing? | IP Routing.” https://www.cloudflare.com/learning/network-layer/what-is-routing/.

·“Costa Rica Declares National Emergency Amid Ransomware Attacks.” The Guardian, 12 May 2022, https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks

·Counter Threat Unit Research Team. “BRONZE STARLIGHT Ransomware Operations Use HUI Loader.” Secureworks, 23 June 2022. https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader.

·Cryakl. “Ransomware-Database/7ev3n/7ev3n-HONE$T at Main · Cryakl/Ransomware-Database.” GitHub, https://github.com/Cryakl/Ransomware-Database/tree/main/7ev3n/7ev3n-HONE%24T.

·Cyber Attacks in Times of Conflict. CyberPeace Institute, https://cyberconflicts.cyberpeaceinstitute.org/.

·Cyber Incident Tracer #HEALTH. CyberPeace Institute, https://cit.cyberpeaceinstitute.org/.

·Cyberdefense, CERT Orange. Cert-Orangecyberdefense/Ransomware_map. 2023. 2025, https://github.com/cert-orangecyberdefense/ransomware_map.

·Cybereason. Cybereason - AI-Driven XDR Platform | MDR | Retainers. https://www.cybereason.com

·CyberPeace Tracer - Cyber Threats and Disinformation Operations Impacting Civil Society. CyberPeace Institute, https://cyberpeacetracer.ngo/analysis

·Cybersecurity Alerts & Advisories. CISA, 17 June 2025, https://www.cisa.gov/news-events/cybersecurity-advisories.

·Cybersecurity That Outmaneuvers Attackers. Redacted, https://redacted.com/

·Darktrace | The Essential AI Cybersecurity Platform. Darktrace, https://www.darktrace.com.

·DeOrio, M. "Temporary disruption or long-term impact: are ransomware takedowns decreasing cybercrime?" SRM Inform, 16 April 2024. https://www.s-rminform.com/cyber-intelligence-briefing/temporary-disruption-or-long-term-impact-are-ransomware-takedowns-decreasing-cybercrime?utm_source

·District of New Jersey. "Russian and Canadian National Charged for Participation in Lockbit Global Ransomware Campaign". United States Department of Justice, 10 Nov. 2022, https://www.justice.gov/usao-nj/pr/russian-and-canadian-national-charged-participation-lockbit-global-ransomware-campaign.

·Europol. "Germany and Ukraine Hit Two High-Value Ransomware Targets – Forensic Analysis of the Seized Equipment Is Still Ongoing to Determine the Exact Role of the Suspects and Their Links to Other Accomplices." https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets.

·Europol. "Internet Organised Crime Threat Assessment (IOCTA) 2023." EUROPOL, 2023, http://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf.

·Europol. "LockBit Power Cut: Four New Arrests and Financial Sanctions against Affiliates – A Developer, a Bulletproof Hosting Service Administrator, and Two Other Associates Arrested in a Series of Coordinated Action by France, the United Kingdom and Spain." Europol, https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates.

·Fadilpasic Sead. "US becomes ransomware capital of the world as attacks rise by almost 150 percent." TechRadar, 4 August 2025. https://www.techradar.com/pro/security/us-becomes-ransomware-capital-of-the-world-as-attacks-rise-by-almost-150-percent.

·FireEye. "Fin10: Anatomy of a Cyber Extortion Operation." FireEye, 2017, http://www.fireeye.com/blog/threat-research/2017/06/fin10-anatomy-of-a-cyber-extortion-operation.html.

·Flare Threat Exposure Management. “Identify Malicious Infrastructure.” 19 May 2025. https://flare.io/glossary/identify-malicious-infrastructure/.

·Geofencing - Unprotect Project. Geofencing, https://unprotect.it/technique/geofencing/.

·“How Operation Cronos Disrupted Ransomware Group LockBit.” World Economic Forum, Feb. 2024, https://www.weforum.org/stories/2024/02/lockbit-ransomware-operation-cronos-cybercrime/

·HHS Office for Civil Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack. US Department of Health and Human Services. https://us.pagefreezer.com/en-US/wa/browse/0a7f82bb-be6e-448a-ae11-373d22c37842?find-by-timestamp=2025-01-02T05:49:59Z&url=https:%2F%2Fwww.hhs.gov%2Fabout%2Fnews%2F2024%2F03%2F13%2Fhhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html&timestamp=2025-01-02T07:03:02Z.

·Hogeveen, Bart. “The UN Norms of Responsible State Behaviour in Cyberspace.” Australian Strategic Policy Institute, 2022, http://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf.

·Infoblox Home. Infoblox Blog, https://blogs.infoblox.com/.

·IP Info. “What Is an IP Netblock? How to Find Netblock Owner? - FAQ & Help Centre - IPinfo.Io,” September 23, 2021. https://ipinfo.io/faq/article/74-what-is-an-ip-netblock-how-to-find-netblock-owner.

·Institute for Security and Technology. “Ransomware Task Force (RTF),” 2021. https://securityandtechnology.org/ransomwaretaskforce/.

·Institute for Security and Technology. “Combating Ransomware: A Comprehensive Framework for Action,” 21 April 2021. https://securityandtechnology.org/virtual-library/report/combating-ransomware-a-comprehensive-framework-for-action/.

·Interpol. “INTERPOL-led operation takes down prolific cybercrime ring”. INTERPOL, 5 Nov. 2021, https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring.

·Jarnecki, Joseph, and Jamie MacColl. “Ransomware Now Threatens the Global South,” August 12, 2022. https://www.rusi.org/explore-our-research/publications/commentary/ransomware-now-threatens-global-south

·Kersten, M. “Read The Manual Locker: A Private RaaS Provider”. Trellix, 2023. https://www.trellix.com/blogs/research/read-the-manual-locker-a-private-raas-provider/.

·Law Enforcement Disrupt World’s Biggest Ransomware Operation. Europol, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.

·LockBit Power Cut: Four New Arrests and Financial Sanctions against Affiliates. Europol https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates.

·Meegan-Vickers, Jack. “The LockBit Takedown: Law Enforcement ‘Trolls’ Ransomware Gang.” Global Initiative, 4 April 2024, https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/.

·Microsoft Threat Intelligence. “Microsoft Digital Defense Report 2024.” Microsoft, 2024, http://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf.

·Murphy, Margi. “Scattered Spider Hacking Suspect Extradited to US From Spain.” Bloomberg.Com, 24 Apr. 2025, https://www.bloomberg.com/news/articles/2025-04-24/scattered-spider-hacking-suspect-extradited-to-us-from-spain.

·Office for Civil Rights (OCR). “Breach Notification Rule.” Page. US Department of Health and Human Services, September 14, 2009. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

·Office of Public Affairs. “Department of Justice Launches Global Action Against NetWalker Ransomware”. United States Department of Justice, 27 Jan. 2021, https://www.justice.gov/archives/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware.

·Office of Public Affairs. “Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant”. United States Department of Justice, 18 Dec. 2023, https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.

·Office of Public Affairs. “Romanian National Sentenced to 20 Years in Prison in Connection with NetWalker Ransomware Attacks”. United States Department of Justice, 19 Dec. 2024, https://www.justice.gov/archives/opa/pr/romanian-national-sentenced-20-years-prison-connection-netwalker-ransomware-attacks

·Office of Public Affairs. “Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses”. United States Department of Justice, 28 Nov. 2018, https://www.justice.gov/archives/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public.

·Office of Public Affairs. “United States Charges Dual Russian and Israeli National as Developer of LockBit Ransomware Group”. United States Department of Justice, 19 Dec. 2024, https://www.justice.gov/archives/opa/pr/united-states-charges-dual-russian-and-israeli-national-developer-lockbit-ransomware-group.

·Perera, David. “NetWalker Ransomware Affiliate Faces 20 Years in US Prison.” BankInfo Security, 5 October 2022, https://www.bankinfosecurity.com/netwalker-ransomware-affiliate-faces-20-years-in-us-prison-a-20215

·Power Rankings: Ransomware Malicious Quartile Q1-2025. Halcyon, https://www.halcyon.ai/raas-mq/power-rankings-ransomware-malicious-quartile-q1-2025.

·Qualys | Expert Network Security Guidance and News. Qualys, https://blog.qualys.com/.

·Ransomware.org. “2024 State of Ransomware: A Revealing Report for IT Professionals by IT Professionals.” Ransomware.Org, 2024, ransomware.org/wp-content/uploads/2024/03/2024-State-of-Ransomware-Report_v1.pdf.

·ReliaQuest | Make Security Possible. ReliaQuest, https://reliaquest.com/.

·Research Blog: Latest Cyber Security Insights. NCC Group, https://www.nccgroup.com/us/research-blog.

·ReversingLabs. “ReversingLabs | Software Supply Chain Security & Threat Intelligence.” ReversingLabs, https://www.reversinglabs.com.

·Reuters. “EU Agency Says Third-Party Ransomware Behind Airport Disruptions.” Reuters, 22 September 2025. https://www.reuters.com/business/aerospace-defense/eu-agency-says-third-party-ransomware-behind-airport-disruptions-2025-09-22/

·Shadowserver Foundation. “Qakbot Botnet Disruption”. 29 August 2023. https://www.shadowserver.org/news/qakbot-botnet-disruption/.

.

·Smeets, Max. “The Ransomware Playbook and How to Disrupt It.” Virtual Routes, 2025, http://virtual-routes.org/wp-content/uploads/2025/03/Virtual-Routes-Pharos-Report-Series_No-1_The-Ransomware-Playbook-and-How-to-Disrupt-It.pdf.

·Sygnia Cybersecurity Services - Beat Attackers and Stay Secure. Sygnia, https://www.sygnia.co/.

·The Latest Ransomware Statistics (Updated June 2025). AAG IT Support. https://aag-it.com/the-latest-ransomware-statistics/.

·The No More Ransom Project. “About the Project.” https://www.nomoreransom.org/en/about-the-project.html.

·The State of Ransomware in 2023. BlackFog, 8 Jan. 2024, https://www.blackfog.com/the-state-of-ransomware-in-2023/.

·Threat Group Cards: A Threat Actor Encyclopedia. APT ETDA, https://apt.etda.or.th/cgi-bin/aptgroups.cgi.

·ThreatFox. https://threatfox.abuse.ch/

·Timokhin, Alexander. “What Are IP Blocks and How Do They Work? - Interlir Networks Marketplace,” September 27, 2024. https://interlir.com/2024/09/27/what-are-ip-blocks-and-how-do-they-work/.

·Trend Micro, https://www.trendmicro.com/it_it/business.html.

·Trend Micro. “Global Operations Lead to Arrests of Alleged Members of GandCrab REvil and Cl0p Cartels”. TrendMicro, 16 Nov. 2021. https://www.trendmicro.com/en_us/research/21/k/global-operations-lead-to-arrests-of-alleged-members-of-gandcrab.html.

·UK Government. “Explaining Uncertainty in UK Intelligence Assessment.” GOV.UK, https://www.gov.uk/government/publications/explaining-uncertainty-in-uk-intelligence-assessment/explaining-uncertainty-in-uk-intelligence-assessment.

·UK National Crime Agency. “Evil Corp: Behind the Screens.” UK National Crime Agency, Oct. 2024, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/732-evil-corp-behind-the-screens/file

·Unit 42 - Latest Cyber Security Research | Palo Alto Networks. Unit 42, 17 June 2025, https://unit42.paloaltonetworks.com/.

·United Nations Department of Economic and Social Affairs. “United Nations International Standard Industrial Classification of All Economic Activities.” United Nations, 2008, ST/ESA/STAT/SER.M/4/Rev.4, http://unstats.un.org/unsd/publication/seriesm/seriesm_4rev4e.pdf.

·United Nations General Assembly (UNGA). “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” United Nations, 22 July 2015, https://docs.un.org/en/A/70/174.

·United Nations General Assembly (UNGA). “Creation of a global culture of cybersecurity and the protection of critical information infrastructures: resolution”, A/RES/58/199. 30 Jan 2004, New York: UN. https://digitallibrary.un.org/record/509571.

·United Nations : Office on Drugs and Crime. “United Nations Convention against Cybercrime. Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crime”. http://www.unodc.org/unodc/en/cybercrime/convention/home.html.

·Vijayan, Jai. “FIN10 Threat Actors Hack and Extort Canadian Mining, Casino Industries.” Dark Reading, 16 June 2017. https://www.darkreading.com/threat-intelligence/fin10-threat-actors-hack-and-extort-canadian-mining-casino-industries.

·VirusTotal - Home. VirusTotal, https://www.virustotal.com/gui/home/search.

·Warminsky, Joe. “Takedown of Lolek Bulletproof Hosting Service Includes Arrests, NetWalker Indictment”. The Record, 11 August 2023, https://therecord.media/five-arrested-in-lolek-takedown.

·World Economic Forum, WEF. “Digital Public Infrastructure Is Key to a Connected Future”, World Economic Forum, 2025, https://www.weforum.org/stories/2025/04/digital-public-infrastructure-building-connected-future/

·World Economic Forum. “Disrupting Cybercrime Networks: A Collaboration Framework.” World Economic Forum, 11 November 2024. https://www.weforum.org/publications/disrupting-cybercrime-networks-a-collaboration-framework/

·Zimmermann, Daniel. “D0glun Ransomware: Analysis & Protection – Gridinsoft Blog.” GridinSoft (blog), 16 April 2025. https://gridinsoft.com/blogs/d0glun-ransomware/.

·Zuckerman, Michael. “DNS Early Detection - Breaking the Black Basta Ransomware Kill Chain | Infoblox.” Infoblox Blog, 1 Aug. 2024, https://blogs.infoblox.com/threat-intelligence/dns-early-detection-breaking-the-black-basta-ransomware-kill-chain/.

Geneva - 2025