**Ewelina Melaniuk**[1]
Akademia Bialska im. Jana Pawł II, Biała Podlaska

https://doi.org/10.29316/9788368103373_18

# TAKSONOMIA INCYDENTÓW RANSOMWARE 2024-2025

## TAXONOMY OF RANSOMWARE INCIDENTS 2024-2025

**Streszczenie**

Ransomware pozostaje jednym z najbardziej dynamicznych zagrożeń w cyberprzestrzeni, a lata 2024-2025 przyniosły nowe, złożone formy ataków, w tym modele Ransomware-as-a-Service (RaaS), podwójne wymuszenia oraz złośliwe oprogramowanie wspomagane sztuczną inteligencją. Celem rozdziału jest opracowanie taksonomii incydentów ransomware w tym okresie. Analiza opiera się na raportach instytucjonalnych, dokumentach branżowych oraz literaturze naukowej. W badaniu wyróżniono cztery wymiary klasyfikacyjne: technikę ataku, wektor początkowego dostępu, strukturę organizacyjną sprawców oraz sektor ofiary. Dyskusja wyników obejmuje przykłady konkretnych incydentów oraz wskazuje na rosnącą adaptacyjność zagrożeń. Opracowana taksonomia może wspierać zespoły SOC, CERT oraz decydentów w monitorowaniu i reagowaniu na incydenty ransomware.

**Słowa kluczowe:** ransomware, taksonomia incydentów, RaaS, podwójne wymuszenia, cyberbezpieczeństwo, analiza zagrożeń

[1] https://orcid.org/0009-0002-9434-6258, e-mail: e.melaniuk@dyd.akademiabialska.pl

**Abstract**

Ransomware remains one of the most dynamic cyber threats, with 2024-2025 witnessing increasingly complex attacks, including Ransomware-as-a-Service (RaaS), double extortion, and AI-assisted malware. The aim of this chapter is to propose a taxonomy of ransomware incidents during this period. The analysis is based on institutional reports, industry documents, and scientific literature. Four classification dimensions were identified: attack technique, initial access vector, organisational structure of perpetrators, and victim sector. The discussion includes concrete examples and highlights the growing adaptability of ransomware threats. The proposed taxonomy can support SOC teams, CERTs, and decision-makers in monitoring and responding to ransomware incidents.

**Keywords:** ransomware, incident taxonomy, RaaS, double extortion, cybersecurity, threat analysis

## Wstęp

Ransomware od ponad dekady pozostaje jednym z najbardziej destrukcyjnych i dynamicznie ewoluujących zagrożeń w cyberprzestrzeni. Jego istota polega na połączeniu technicznych mechanizmów sabotażu informacyjnego z klasycznym wymuszeniem finansowym, co czyni go szczególnie skutecznym narzędziem cyberprzestępczym (ENISA, 2024). W latach 2024-2025 zagrożenie to nie tylko nie uległo osłabieniu, lecz przyjęło nowe, bardziej złożone formy organizacyjne i technologiczne, obejmujące m.in. model Ransomware-as-a-Service (RaaS), strategię podwójnego i potrójnego wymuszenia oraz coraz częstsze wykorzystanie narzędzi sztucznej inteligencji (IBM Security, 2024; Raz i in., 2025).

Zgodnie z danymi przedstawionymi w raporcie *Worldwide Ransomware 2024*, liczba globalnych incydentów ransomware w 2024 r. utrzymywała się na wysokim poziomie, pomimo intensyfikacji działań organów ścigania oraz międzynarodowych operacji wymierzonych w infrastrukturę przestępczą (Cyber Threat Intelligence Integration Center [CTIIC], 2025). Jednocześnie w 2025 r. zaobserwowano dalszą fragmentację ekosystemu ransomware, polegającą na wzroście liczby mniejszych, krótkotrwałych grup przestępczych, co znacząco utrudnia ich identyfikację i neutralizację (ESET, 2025). Istotnym problemem badawczym pozostaje brak jednolitej, aktualnej taksonomii incydentów ransomware, która uwzględniałaby współczesne

kryteria klasyfikacyjne, takie jak technika ataku, wektor początkowego dostępu, struktura organizacyjna sprawców czy sektor ofiary. Dotychczasowe ujęcia koncentrowały się głównie na aspektach technicznych złośliwego oprogramowania, pomijając kontekst operacyjny i ekonomiczny ataków (ENISA, 2024). Tymczasem raporty branżowe wskazują, że skuteczna analiza i reagowanie na incydenty ransomware wymagają podejścia wielowymiarowego, łączącego perspektywę techniczną, organizacyjną oraz sektorową (IBM Security, 2024).

Celem niniejszego rozdziału jest zaproponowanie systematycznej taksonomii incydentów ransomware z lat 2024-2025, która umożliwi uporządkowanie obserwowanych zjawisk oraz identyfikację dominujących trendów zagrożeń. Przyjęta klasyfikacja opiera się na analizie raportów instytucji międzynarodowych, firm zajmujących się cyberbezpieczeństwem oraz literatury naukowej, w tym najnowszych badań dotyczących automatyzacji i wykorzystania modeli językowych w tworzeniu złośliwego oprogramowania (CTIIC, 2025, Raz i in., 2025). Wyniki zaproponowanej taksonomii mogą stanowić istotne wsparcie dla zespołów SOC, CERT oraz decydentów odpowiedzialnych za zarządzanie ryzykiem cybernetycznym, a także przyczynić się do dalszych badań nad predykcją i ograniczaniem skutków ataków ransomware w środowiskach krytycznych.

## Metodologia badań

W niniejszym rozdziale zastosowano jakościowo-ilościowe podejście badawcze, którego celem było opracowanie aktualnej i wielowymiarowej taksonomii incydentów ransomware w latach 2024-2025. Metodologia opiera się na analizie wtórnej danych pochodzących z raportów instytucjonalnych, dokumentów branżowych oraz literatury naukowej, co jest powszechnie stosowaną praktyką w badaniach nad zagrożeniami cybernetycznymi (ENISA, 2024).

Podstawowym źródłem danych były raporty o zagrożeniach ransomware publikowane przez instytucje międzynarodowe oraz firmy zajmujące się cyberbezpieczeństwem, w szczególności: raport *Worldwide Ransomware 2024* przygotowany przez Cyber Threat Intelligence Integration Center (CTIIC, 2025), *ENISA Threat Landscape 2024*, *IBM X-Force Threat Intelligence Index 2024* i raporty analityczne ESET z 2025 r. Źródła te zostały

wybrane ze względu na ich wysoką wiarygodność, cykliczność publikacji oraz szeroki zakres danych empirycznych, obejmujących analizę techniczną incydentów, a także kontekst organizacyjny i sektorowy (IBM Security, 2024; ESET, 2025).

Uzupełniająco wykorzystano publikacje naukowe, w tym prace poświęcone automatyzacji ataków i zastosowaniu sztucznej inteligencji w cyberprzestępczości, co pozwoliło na identyfikację nowych kategorii zagrożeń, takich jak ransomware wspomagane przez modele językowe (Raz i in., 2025).

Proces badawczy składał się z czterech etapów:

1. Selekcja i normalizacja danych – wyodrębniono opisy incydentów ransomware z lat 2024-2025, eliminując duplikaty oraz przypadki niejednoznacznie zaklasyfikowane w źródłach pierwotnych (CTIIC, 2025).
2. Analiza porównawcza – przeprowadzono porównanie sposobów klasyfikacji stosowanych w poszczególnych raportach, identyfikując wspólne oraz rozbieżne kryteria opisu incydentów (ENISA, 2024).
3. Kodowanie kategorii – na podstawie analizy jakościowej wyodrębniono kluczowe zmienne klasyfikacyjne, takie jak: technika ataku, wektor początkowego dostępu, model organizacyjny sprawców, sektor ofiary oraz potencjalny wpływ incydentu. Takie podejście odpowiada rekomendacjom dotyczącym badań nad złożonymi zagrożeniami cybernetycznymi (IBM Security, 2024).
4. Synteza i budowa taksonomii – na podstawie zakodowanych danych zaproponowano spójną strukturę taksonomiczną, umożliwiającą jednoczesną analizę techniczną i kontekstową incydentów ransomware (ENISA, 2024).

W części ilościowej wykorzystano analizę częstości występowania poszczególnych typów incydentów oraz trendów czasowych, zgodnie z danymi zagregowanymi w raportach branżowych (ESET, 2025). Część jakościowa obejmowała analizę treści opisów incydentów oraz strategii grup ransomware, co pozwoliło na identyfikację nowych wzorców działania, w tym fragmentacji grup przestępczych i adaptacyjnych modeli RaaS (CTIIC, 2025).

Zastosowana metodologia opiera się na danych wtórnych, co oznacza zależność od zakresu i jakości raportów źródłowych. Ponadto, ze względu na

niejawny charakter wielu incydentów ransomware, rzeczywista skala zjawiska może być niedoszacowana (ENISA, 2024). Niemniej jednak triangulacja źródeł pozwala na zwiększenie rzetelności i wiarygodności zaproponowanej taksonomii (IBM Security, 2024).

## Wyniki i dyskusja

Analiza danych z lat 2024-2025 pozwoliła na wyodrębnienie kilku kluczowych kategorii incydentów ransomware oraz identyfikację dominujących trendów w tym okresie. Na podstawie raportów CTIIC (2025), ENISA (2024), IBM Security (2024) oraz ESET (2025) opracowano taksonomię obejmującą cztery wymiary klasyfikacyjne: technikę ataku, wektor początkowego dostępu, strukturę organizacyjną sprawców oraz sektor ofiary.

## Technika ataku

Technika ataku definiuje sposób działania ransomware w systemach ofiary. Obejmuje metody szyfrowania danych, strategie wymuszeń oraz adaptacje do systemów obronnych. Analiza incydentów z lat 2024-2025 wskazuje, że współczesne ransomware ewoluuje w kierunku coraz bardziej złożonych i wielowarstwowych technik.

1. Encryption ransomware (szyfrujące).

Klasyczny wariant ransomware, w którym złośliwe oprogramowanie szyfruje pliki ofiary, uniemożliwiając dostęp do danych bez zapłaty okupu, nadal pozostaje istotnym zagrożeniem. Przykład stanowi atak grupy Conti na amerykańską firmę logistyczną w 2024 r., gdzie zaszyfrowano systemy magazynowe, powodując poważne zakłócenia w łańcuchu dostaw. Incydent ten pokazuje, że nawet w przypadku tradycyjnych technik, skala i precyzja ataków mogą generować ogromne straty finansowe i operacyjne (ENISA, 2024).

2. Double extortion ransomware (podwójne wymuszenie).

Wariant podwójnego wymuszenia stał się dominujący w 2024-2025 r. Atakujący nie tylko szyfrują dane, ale również kradną wrażliwe informacje i grożą ich ujawnieniem w przypadku braku zapłaty, zwiększając presję na ofiarę. Przykładem jest incydent grupy LockBit na rumuński szpital w 2025 r., gdzie oprócz szyfrowania dokumentacji medycznej, sprawcy grozili publikacją danych pacjentów w sieci. Ten typ ataku pokazuje rosnącą

rolę strategii psychologicznych w wymuszaniu okupu oraz potrzebę rozbudowanych procedur bezpieczeństwa danych (IBM Security, 2024).

3. AI-assisted ransomware (wspomagane sztuczną inteligencją).

Nowoczesne kampanie ransomware wykorzystują sztuczną inteligencję do automatyzacji ataków i generowania spersonalizowanego phishingu. W 2025 r. eksperymentalne kampanie w USA wykazały, że AI mogła tworzyć e-maile phishingowe dostosowane do profili zawodowych pracowników korporacji finansowej, zwiększając skuteczność infekcji. Ransomware wspomagany AI może również adaptować swoje działanie w czasie rzeczywistym, np. omijać antywirusy i systemy monitoringu, co podkreśla rosnącą złożoność i trudność w wykrywaniu takich zagrożeń (Raz i in., 2025).

4. Multi-stage attacks (wieloetapowe ataki).

W 2024-2025 r. coraz częściej obserwowano wieloetapowe kampanie, w których ransomware był tylko jednym z elementów ataku. Przykładem jest kampania grupy Akira w Hiszpanii, w której najpierw włamano się do systemu poprzez niezaktualizowaną podatność, następnie przejęto konta administracyjne, a dopiero w końcowej fazie wprowadzono złośliwe oprogramowanie szyfrujące dane. Takie podejście umożliwia sprawcom maksymalizację zysków oraz minimalizację ryzyka wykrycia w początkowych etapach ataku (ENISA, 2024).

5. Targeted ransomware campaigns (atakowane precyzyjnie sektory).

Coraz częściej obserwuje się ataki skoncentrowane na określonych sektorach, np. szpitalach, administracji publicznej czy instytucjach edukacyjnych. Przykład: atak grupy REvil na uniwersytet w Wielkiej Brytanii w 2024 r., w którym ransomware został dostosowany do środowiska sieciowego uczelni i zabezpieczeń serwerów. Skierowane kampanie pozwalają sprawcom zoptymalizować kod malware, zwiększając jego skuteczność i maksymalizując straty ofiary (ESET, 2025).

Analiza wskazuje, że współczesne ransomware nie jest już jednorodnym zagrożeniem. Trendy w latach 2024-2025 pokazują:

- rosnącą rolę strategii podwójnego wymuszenia i presji psychologicznej na ofiarach,
- wprowadzenie AI i automatyzacji w procesach ataków, zwiększających skuteczność i adaptacyjność malware,

- coraz częstsze stosowanie wieloetapowych kampanii i technik hybrydowych, łączących phishing, eksploatację podatności i przejęcie poświadczeń,
- dopasowanie ataków do specyfiki sektorów ofiary, co zwiększa ich skuteczność i skalę strat (ENISA, 2024; IBM Security, 2024; Raz i in., 2025).

Wyniki te podkreślają, że skuteczna obrona wymaga wielowarstwowej ochrony, obejmującej systemy detekcji i reakcji, edukację użytkowników, szybkie aktualizacje oprogramowania oraz monitorowanie hybrydowych i zautomatyzowanych ataków.

## Wektor początkowego dostępu

Wektor początkowego dostępu to metoda, za pomocą której ransomware infiltruje system ofiary, inicjując cały proces ataku. Analiza danych z lat 2024-2025 wskazuje, że pomimo rozwoju technik obronnych nadal phishing i spear-phishing pozostają dominującymi punktami wejścia, odpowiadającymi za 38-40% wszystkich incydentów (ESET, 2025). Przykładem jest atak grupy REvil na firmę usługową w Wielkiej Brytanii w 2024 r., w którym pracownik nieświadomie otworzył złośliwy link w e-mailu podszywającym się pod komunikat bankowy, umożliwiając zainstalowanie się ransomware na firmowych serwerach. Incydent ten ilustruje, że techniki socjotechniczne pozostają skuteczne nawet w organizacjach z częściową świadomością zagrożeń.

Drugim istotnym wektorem są ataki oparte na eksploatacji podatności w systemach i aplikacjach, w tym zarówno tzw. zero-day, jak i n-day vulnerabilities. W 2024 r. grupa Akira przeprowadziła atak na administrację miejską w Hiszpanii, wykorzystując niezaktualizowaną podatność w oprogramowaniu serwera WWW, co pozwoliło na zdalną instalację ransomware i szyfrowanie danych krytycznych. Ten przypadek pokazuje, że brak systematycznej aktualizacji systemów operacyjnych i aplikacji stanowi wciąż istotny punkt wejścia dla cyberprzestępców (ENISA, 2024).

Kolejnym coraz częściej wykorzystywanym kanałem jest kompromitacja poświadczeń, w tym ataki typu brute force lub credential stuffing na zdalny dostęp (RDP, VPN). Przykład ataku na szpital w USA w 2025 r. pokazuje, że przejęcie loginów administratora VPN umożliwiło sprawcom

nieograniczony dostęp do wewnętrznych sieci i danych pacjentów, co podkreśla znaczenie silnej polityki haseł oraz mechanizmów uwierzytelniania wieloskładnikowego (IBM Security, 2024).

W ostatnich latach wyraźnie wzrasta znaczenie ataków poprzez łańcuchy dostaw i dostawców usług trzecich. Przykładem jest incydent w 2025 r., w którym atak na dostawcę oprogramowania księgowego doprowadził do infekcji ransomware u kilkudziesięciu klientów firmy. Ten przypadek pokazuje, że współczesne zagrożenia są coraz bardziej powiązane z globalnymi sieciami powiązań biznesowych i że bezpieczeństwo organizacji nie zależy wyłącznie od własnych systemów, ale także od zabezpieczeń partnerów i dostawców (CTIIC, 2025).

## Struktura organizacyjna sprawców

Analiza struktury sprawców ransomware w latach 2024-2025 pokazuje, że rynek cyberprzestępczy pozostaje zróżnicowany i dynamiczny. Dominują wciąż duże, zorganizowane grupy ransomware, takie jak LockBit i Akira, prowadzące długofalowe, kompleksowe kampanie ataków. Przykładem jest kampania LockBit 3.0 w USA w 2024 r., obejmująca kilkadziesiąt instytucji finansowych i usługowych. Incydent ten pokazał profesjonalizację tych grup, w tym posiadanie dedykowanych zespołów ds. programowania malware, działów marketingu w celu koordynowania afiliacji i skutecznego egzekwowania wymuszeń finansowych. Skala i precyzja ataku dowodzą, że nowoczesne grupy ransomware funkcjonują niemal jak legalne przedsiębiorstwa o rozbudowanej strukturze operacyjnej (CTIIC, 2025).

Jednocześnie rozwój modelu Ransomware-as-a-Service (RaaS) umożliwia mniej doświadczonym przestępcom przeprowadzanie ataków na szeroką skalę, co w praktyce oznacza demokratyzację narzędzi przestępczych. Przykład RaaS „Hive" w 2025 r. pokazuje, że nawet pojedynczy afiliant w Europie lub Ameryce Południowej mógł przeprowadzić atak na szkoły, małe przedsiębiorstwa i instytucje kulturalne, przy czym twórcy RaaS pobierali procent od okupów. Ten model zwiększa globalną penetrację rynku ransomware, a jednocześnie utrudnia identyfikację faktycznych sprawców, ponieważ grupa tworząca malware i grupa realizująca atak mogą być całkowicie oddzielne (ENISA, 2024).

Kolejnym istotnym trendem jest wzrost liczby małych, efemerycznych grup przestępczych, takich jak CyberVolk w Niemczech w 2025 r. Takie grupy działają sezonowo, przez kilka tygodni lub miesięcy, celując w lokalne przedsiębiorstwa i wykorzystując luki w zabezpieczeniach często niedostrzegane przez większe grupy. Fragmentacja rynku sprawców zwiększa trudność w monitorowaniu zagrożeń oraz wymaga od zespołów bezpieczeństwa adaptacyjnych strategii reagowania, które obejmują szybką identyfikację nowych podmiotów oraz aktualizację reguł detekcji (ESET, 2025; Raz i in., 2025). Dodatkowo w literaturze wskazuje się na elastyczne i hybrydowe struktury organizacyjne, w których grupy RaaS współpracują z niezależnymi programistami malware, ekspertami od phishingu i brokerami danych. Taka modularna organizacja umożliwia szybkie skalowanie kampanii, testowanie nowych technik ataku i szybką adaptację do działań organów ścigania. Przykładem jest międzynarodowa kampania LockBit w 2024 r., w której do ataków użyto afiliantów w Europie Wschodniej i Ameryce Północnej, a infrastruktura do wymuszeń była koordynowana centralnie przez grupę macierzystą (CTIIC, 2025).

Wnioski płynące z obserwacji struktury sprawców wskazują, że skuteczna obrona wymaga ścisłego monitorowania ekosystemu cyberprzestępczego, w tym rozpoznawania nowych grup RaaS, śledzenia afiliantów oraz reagowania na hybrydowe modele ataków. Zrozumienie organizacyjnej dynamiki sprawców pozwoli przewidywać skalę i kierunki ataków oraz opracowywać strategie prewencji i wczesnego ostrzegania dla instytucji publicznych i prywatnych.

## Sektor ofiary

Analiza sektorów ofiar w latach 2024-2025 wskazuje, że największe zagrożenie dotyczy infrastruktury krytycznej, administracji publicznej i sektora edukacyjnego. Przykładem jest atak na rumuńską stację wodociągową w 2025 r., w wyniku którego tymczasowo wstrzymano dystrybucję wody w kilku miastach. Incydent ten podkreśla wysokie potencjalne skutki społeczne ransomware'u i istotną rolę infrastruktury krytycznej w funkcjonowaniu państwa i społeczeństwa (ENISA, 2024). Podobnie w sektorze energetycznym, ataki na lokalne elektrownie i sieci przesyłowe wykazały, że

ransomware może sparaliżować systemy zarządzania, powodując przestoje produkcji i ryzyko dla bezpieczeństwa publicznego (CTIIC, 2025).

W sektorze prywatnym ransomware powoduje poważne straty finansowe i operacyjne, szczególnie w przedsiębiorstwach logistycznych, produkcyjnych i finansowych. Atak na firmę logistyczną w USA w 2025 r. doprowadził do zatrzymania systemów magazynowych i spedycyjnych, generując straty liczone w milionach dolarów. W takich przypadkach konieczne były również pilne inwestycje w systemy bezpieczeństwa IT oraz audyty infrastruktury, co pokazuje długofalowy koszt incydentów (IBM Security, 2024).

Nowym trendem w latach 2024-2025 jest celowanie w instytucje kultury, badań i archiwa cyfrowe, które dotychczas były traktowane jako mniej atrakcyjne cele. Przykładem jest atak na bibliotekę narodową w Europie Środkowej w 2025 r., gdzie zaszyfrowano katalogi cyfrowe i dokumenty historyczne. Atak ten pokazuje, że cyberprzestępcy rozszerzają pole działania na podmioty, które posiadają wartościowe zasoby, ale często dysponują słabszymi mechanizmami ochrony (ESET, 2025). Dodatkowo w literaturze branżowej zauważono rosnącą liczbę ataków sektorowo ukierunkowanych, w których ransomware jest dostosowany do specyfiki infrastruktury ofiary. Przykładem jest kampania grupy LockBit 3.0 w 2024 r., skierowana do instytucji edukacyjnych i uczelni wyższych w Europie, gdzie kod malwaru był zoptymalizowany do działania w środowisku sieciowym kampusów, omijając standardowe zabezpieczenia serwerów edukacyjnych. Takie celowane podejście pozwala sprawcom na zwiększenie skuteczności ataków oraz maksymalizację presji finansowej na ofiary (ENISA, 2024; IBM Security, 2024).

Analiza sektorów ofiar wskazuje, że różnorodność celów rośnie, a nowoczesne kampanie ransomware nie ograniczają się już do dużych firm czy instytucji publicznych. Zrozumienie specyfiki ataków w poszczególnych sektorach umożliwia priorytetyzację zasobów obronnych i opracowanie strategii prewencji dostosowanej do rodzaju działalności, potencjalnych strat i wartości danych (CTIIC, 2025; ESET, 2025).

## Dyskusja i wnioski

Wyniki badań wskazują, że zagrożenia ransomware w latach 2024-2025 cechują się wielowymiarową dynamiką, obejmującą ewolucję

techniczną i zmiany w strukturze organizacyjnej sprawców. Wyodrębnione w rozdziale kategorie klasyfikacyjne – technika ataku, wektor początkowego dostępu, struktura przestępcza oraz sektor ofiary – pozwalają uporządkować istniejące incydenty i jednocześnie identyfikować predyktory przyszłych zagrożeń, takie jak rosnące wykorzystanie sztucznej inteligencji w kampaniach ransomware czy fragmentacja ekosystemu przestępczego (ENISA, 2024; Raz i in., 2025).

Analiza wskazuje, że techniki ataku ewoluują w kierunku podwójnych i zautomatyzowanych wymuszeń. Ataki typu double extortion, w których oprócz szyfrowania danych następują kradzież i groźba publikacji, stają się standardem w działaniach grup takich jak LockBit czy Conti (IBM Security, 2024). W 2025 r. pojawienie się AI-assisted ransomware umożliwiało automatyzację generowania spersonalizowanych wiadomości phishingowych i adaptacyjne omijanie systemów ochrony, co zwiększa skuteczność ataków i trudność w ich wykrywaniu (Raz i in., 2025).

Wektory początkowego dostępu również stają się coraz bardziej złożone. Phishing, wykorzystanie podatności w systemach (zero-day i n-day) oraz ataki przez łańcuchy dostaw i dostawców usług trzecich umożliwiają sprawcom różnorodne ścieżki infiltracji, co zwiększa skuteczność kampanii ransomware i utrudnia obronę (CTIIC, 2025; ESET, 2025). Przykłady ataków na dostawcę oprogramowania księgowego w 2025 r. pokazują, że nawet organizacje o wysokim poziomie zabezpieczeń mogą zostać dotknięte pośrednio przez słabsze ogniwa w globalnych sieciach biznesowych.

Struktury sprawców stają się coraz bardziej zróżnicowane i elastyczne. Dominują duże, profesjonalne grupy, takie jak LockBit i Akira, prowadzące długofalowe kampanie, a także mniejsze, efemeryczne podmioty działające sezonowo, często korzystające z modeli RaaS (ENISA, 2024; ESET, 2025). Fragmentacja ekosystemu sprawców zwiększa trudność monitorowania i wymaga od zespołów SOC i CERT szybkiej adaptacji, np. poprzez śledzenie afiliantów RaaS i identyfikowanie nowych grup przestępczych.

Sektor ofiary determinuje charakter strat i skutki społeczne incydentów. W przypadku infrastruktury krytycznej, stacji wodociągowych czy elektrowni ransomware może prowadzić do zakłóceń w dostępie do podstawowych usług publicznych (ENISA, 2024). W sektorze prywatnym skutki są przede wszystkim finansowe, np. w ataku na firmę logistyczną w USA

w 2025 r., gdzie zatrzymanie systemów spedycyjnych wygenerowało straty liczone w milionach dolarów (IBM Security, 2024). Warto również zauważyć trend atakowania instytucji kultury i badań, takich jak biblioteki cyfrowe, gdzie straty mają charakter niematerialny, ale o dużej wartości historycznej i edukacyjnej (ESET, 2025).

Taksonomia opracowana w rozdziale stanowi narzędzie praktyczne dla zespołów SOC i CERT, umożliwiające skuteczniejsze monitorowanie, klasyfikowanie i raportowanie incydentów ransomware. Może również służyć jako podstawa dla badań prognostycznych, pozwalających przewidywać kierunki rozwoju zagrożeń i identyfikować potencjalne cele ataków (Raz i in., 2025; ESET, 2025).

Wyniki badań podkreślają również konieczność kompleksowego podejścia do zarządzania ryzykiem cybernetycznym, obejmującego:

- wdrożenie i aktualizację oprogramowania zabezpieczającego,
- edukację użytkowników i szkolenia z zakresu bezpieczeństwa informacji,
- monitorowanie łańcuchów dostaw i bezpieczeństwa partnerów biznesowych,
- współpracę międzynarodową oraz wymianę informacji wywiadowczych między podmiotami publicznymi i prywatnymi.

Tylko strategia wielowarstwowa, uwzględniająca aspekty techniczne i organizacyjne, może skutecznie ograniczyć ryzyko i konsekwencje ataków ransomware, zwłaszcza w sektorach najbardziej narażonych (CTIIC, 2025; ENISA, 2024; IBM Security, 2024).

## Podsumowanie wniosków

1. Ransomware rozwija się w kierunku podwójnych wymuszeń i automatyzacji, w tym z użyciem AI.
2. Wektory początkowego dostępu są coraz bardziej złożone i obejmują phishing, podatności systemowe oraz łańcuchy dostaw.
3. Struktury sprawców są zróżnicowane – od dużych, profesjonalnych grup po efemeryczne podmioty korzystające z RaaS.
4. Sektor ofiary determinuje charakter strat i wymusza różne strategie obrony.

5. Kompleksowa strategia ochrony obejmująca technologie, edukację, monitoring partnerów oraz współpracę międzynarodową jest kluczowa dla ograniczenia skutków incydentów.

## Literatura

1. Cyber Threat Intelligence Integration Center. (2025). *Worldwide ransomware, 2024: Increasing rate of attacks tempered by law enforcement disruptions.* Office of the Director of National Intelligence. Pobrane z: https://www.dni.gov/files/CTIIC/documents/products/Worldwide_Ransomware_2024.pdf (dostęp: 22.02.2026).
2. ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. Pobrane z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (dostęp: 22.02.2026).
3. ESET. (b.d.). *Polska najczęściej na świecie atakowana ransomware w 2025 roku.* Pobrane z: https://www.eset.com/pl/about/newsroom/press-releases/news/polska-najczesciej-na-swiecie-atakowana-ransomware-w-2025-roku/ (dostęp: 22.02.2026).
4. IBM Security. (2024). *X-Force threat intelligence index 2024. IBM Corporation*. Pobrane z: https://www.ibm.com/reports/threat-intelligence (dostęp: 22 lutego 2026).
5. Raz, M., Udeshi, M., Sai Charan, P. V., Krishnamurthy, P., Khorrami, F., Karri, R. (2025). *Ransomware 3.0: Self-composing and LLM-orchestrated. arXiv.* https://doi.org/10.48550/arXiv.2508.20444