**2024 rokiem ransomware. Polskie instytucje na celowniku i rekordowe wzrosty za sprawą usług hakerskich!**

**W roku 2024 odnotowano 5414 ataków ransomware na organizacje na całym świecie, co stanowi wzrost aż o 11%. Choć pocztek 2024 roku okazał się spokojny, to cyberprzestępcy wzmożyli aktywność w drugiej połowie roku, a IV kw. 2024 okazał się najbardziej intensywnym okresem, odnotowując 1827 incydentów, co stanowi 1/3 wszystkich ataków w 2024 roku – ujawnia raport Cyberint, należącej do Check Point Software firmy specjalizującej się w wykrywaniu i łagodzeniu skutków cyberataków.**

Wzmożone działania organów ścigania przeciwko dużym grupom ransomware, jak LockBit w lutym 2024 roku, doprowadziły do aresztowań, ujawnienia tożsamości liderów grup oraz przejęcia infrastruktury cyberprzestępczej. Doprowadziło to do rozpadu wielu doświadczonych grup, z których wyłoniło się 46 nowych, w tym RansomHub, który przewyższył aktywnością LockBit. Ogółem liczba znanych i aktywnych grup wzrosła o 40% z 68 w 2023 roku do 95 w 2024 roku.

Z danych należącej do Check Pointa firmy wynika, że najczęściej atakowanym krajem pozostały Stany Zjednoczone z łączną ilością 936 ataków. W czwartym kwartale Indie odnotowały 44 ataki ransomware, co może wskazywać na rosnącą podatność na tego rodzaju zagrożenia.

W Polsce na przestrzeni 2024 roku hakerzy atakowali m.in. administrację publiczną. Grupy ransomware zaatakowały takie podmioty jak Starostwo Powiatowe w Świebodzinie (maj 2024, Play), Powiatowy Urząd pracy w Policach (sierpień 2024, RansomHub). Jak ocenia [portal CyberDefence24](https://cyberdefence24.pl/cyberbezpieczenstwo/najwazniejsze-incydenty-w-2024-roku), najgroźniejszym atakiem w 2024 r. mogła okazać się rzekoma kradzież danych osobowych (m.in. adresów zamieszkania czy numerów PESEL) 80 tys. mieszkańców powiatu jędrzejowskiego. Portal kontaktował się w listopadzie ze Starostwem, jednak **wówczas nie określono tego, czy dane mieszkańców powiatu zostały wykradzione przez RansomHub. W tym czasie cyberprzestępcy usunęli post informujący o ataku oraz nie opublikowali wykradzionych danych.**

Pod względem sektorów najczęściej atakowane były: usługi biznesowe z 451 atakami, handel detaliczny oraz przemysł produkcyjny z 201 atakami w IV kwartale. Co ciekawe, najwyższy wzrost ataków odnotowało budownictwo. Ataków ransomware na ten sektor było w zeszłym roku o 50% więcej w porównaniu z 2023 rokiem.

Grupami o największej aktywności w 2024 roku były RansomHub (531 ataków), LockBit, Play, Akira, IncRansom i Medusa. Dziesięć najaktywniejszych grup było odpowiedzialnych za ponad połowę (52,8%) wszystkich ataków w 2024 roku!

Wzrost ataków ransomware w 2024 roku wynikał przede wszystkim z modelu Ransomware-as-a-Service (RaaS, ang. ransomware jako usługa), który umożliwia nawet niedoświadczonym cyberprzestępcom przeprowadzanie zaawansowanych ataków. Fragmentacja dużych grup doprowadziła do powstania mniejszych, bardziej dynamicznych, co zwiększyło konkurencję i innowacyjność wśród cyberprzestępców. Dodatkowo, ewolucja technik ataków objawiła się wzrostem liczby ataków na systemy Linux i VMware ESXi oraz wykorzystywaniem narzędzi chmurowych do kradzieży danych.

Rok 2024 pokazał, że ewolucja zagrożeń wymaga ciągłego dostosowywania strategii obronnych. Organizacje muszą pozostać czujne i wdrażać wielowarstwowe podejście do cyberbezpieczeństwa, aby skutecznie przeciwdziałać rosnącym zagrożeniom.

Eksperci Cyberint zalecają, by w celu ochrony przed atakami ransomware, organizacje wdrażały zaawansowaną detekcję zagrożeń, zapewniającą bieżący monitoring aktywności sieciowej. Niezbędne jest również regularne aktualizowanie systemów, szczególnie w środowiskach Linux i VMware, aby eliminować znane luki w zabezpieczeniach. Ważnym elementem okazuje się także szkolenie pracowników w zakresie rozpoznawania prób phishingu, a współpraca z innymi organizacjami i organami ścigania może wspomóc wymianę informacji o zagrożeniach.