

Estado del Ransomware en 2024

General

Reporte ThreatDown

Periodo del reporte Julio 2023 a Junio 2024

Los ataques de Ransomware se siguen incrementando anualmente al 33%

Cambio de un numero pequeno de grandes actores, a un gran numero de pequeños actores

Los ataques de ransomware son mas faciles. Se ha reducido la barrera de entrada para los delincuentes.

Los ataques ejecutados por actores que no pertenecen al top 15 aumento de un 25% al 31%

Los pagos recolectados por los actores de Ransomware ya sobrepasaron el \$1 billion de dolares en 2023

Pago promedio de un ataque de ransomware es de \$620,000 dolares

El costo promedio de la recuperacion de un ataque de ransomware equivale a \$4.7 millones de dolares

Por Pais

La actividad del Ransomware se incremento en todos los paises

USA

El 48% de todos los ataques de ransomware del mundo tienen como objetivo USA

Se observo un incremento del 63% en ataques

Epicentro de la actividad de ransomware

Sector salud y educacion son objetivos principales

Su sector educacion sufre el 60% de los ataques mundiales

Su sector salud sufre el 71% de los ataques mundiales

Resto del mundo

UK vio un aumento del 67% en ataques

El sector salud y educacion no parece ser un objetivo prioritario para los atacantes

Por Industria

Manufactura

Se continua viendo un aumento del 71% anual de ataques de ransomware en el sector

Se distribuye por todos los diferentes actores

El aumento se puede explicar por la transformación digital del sector.

La ciberseguridad debe estar integrada en la transformación digital desde el principio

Educacion

Salud

Solo son objetivos relevantes en USA

Tendencias del Ransomware

Incremento en ataques nocturnos

Nocturno+ Madrugada + Fines de semana + feriados

Especialmente desde las 1 am hasta las 5 am

Los ataques se volvieron mas rapidos

La cadena de ataque del ransomware paso de semanas a ser ejecutada en horas

Aumento del uso de tecnicas LOTL

Las herramientas LOTL (Living Off the Land) son herramientas que ya existen y son comunes en el entorno de la victima, ejemplo de estos son: powershell, WMI o el uso de tecnicas como Binary planting.

Actores usa esto para disminuir la deteccion

Los grandes actores ya usan estas tecnicas en su cadena de ataque