halcyon

RaaS VS SaaS

Ransomware is one of the biggest threats to any organization, regardless of size or industry. The downstream impacts from a large-scale ransomware event can have a massive fiscal fallout and real-world repercussions.

Traditional security solutions, while robust and effective for some threats, have clearly failed to protect organizations against ransomware attacks. There is a huge gap in protection and ransomware operators are expertly exploiting it to the tune of hundreds of millions of dollars yearly.

The average cost of remediating a ransomware attack in 2022

$4,500,000.00

That does not include additional costs like:

Ransom Payments
Double Extortion

Increasing Insurance
Premiums

Lost Revenue
Due to Downtime

Brand, Stock and
Reputation Damage

Ransomware Operators are operating akin to a SaaS Organization

Financially Motivated and Driven by Profits

Top-Down Corporate Organizational Structure

Partner Program to Expand Footprint

24/7 Online Customer Support

New Features and Bug Fixes Released Regularly

Leverages Modern Software Development Tools

So Why is Ransomware So Successful?

The Ransomware-as-a-Service (RaaS) business model includes many aspects that mirror legitimate Software-as-a-Service (SaaS) models, making the ransomware game highly profitable.

In fact, if you compare P&L sheets from the leading ransomware operations against leading security solution providers, you'd see ransomware gangs enjoy operating margins that would make almost any SaaS provider envious. RaaS operators are also better viewed as mature criminal business organizations with top-down hierarchical structures and diversified revenue streams.

Organized like a SaaS company

Efficient Marketing and Partner Programs

Multiple Revenue Sharing Options

High Revenue, Low COGS

The RaaS Ecosystem

The ransomware ecosystem has exploded in recent years with many stunning similarities to non-criminal emerging market sectors. This evolution includes the advent of specialists who focus on particular aspects of the ransomware economy who together represent the entire ransomware attack supply chain.

Key players in the ransomware economy include:

Initial Access Brokers

- Compromise the networks of high value target
- May exploit access themselves for various criminal activities
- May exhibit attack infrastructure crossover with nation-state attackers
- Sells access to other attackers, including ransomware affiliates

RaaS Platform Providers

- Develops ransomware attack platform, attack toolkits
- Manages C2 infrastructure, payment portal, leak site
- Assists with ransom negotiations, payment processing and laundering
- Markets to platform to affiliates, provides technical support

Affiliates and Partners

- Rent RaaS platform and splits proceeds with RaaS developer
- Sets targets, ransom demand, post-infection messaging
- Initiates and manages the ransomware attack campaigns

Crypto Money Launderers

- Specialize in leveraging crypto exchanges to hide and launder illegal funds
- Move finds between wallets, across crypto currencies, or into other asset types
- Abuse DeFi's/Dex's (decentralized finance/exchanges) to mask funds

Manages decryption keys and post-infection actions

Favor difficult to trace blockchains like Monero and ZCash

RaaS

A Buyer's Market

6,300+
active Dark Web Markets as of 2022

Largest 2022 payment:
$40M

Ransomware kits starting as low as
$10.05

Unique ransomware product offerings
45,000+

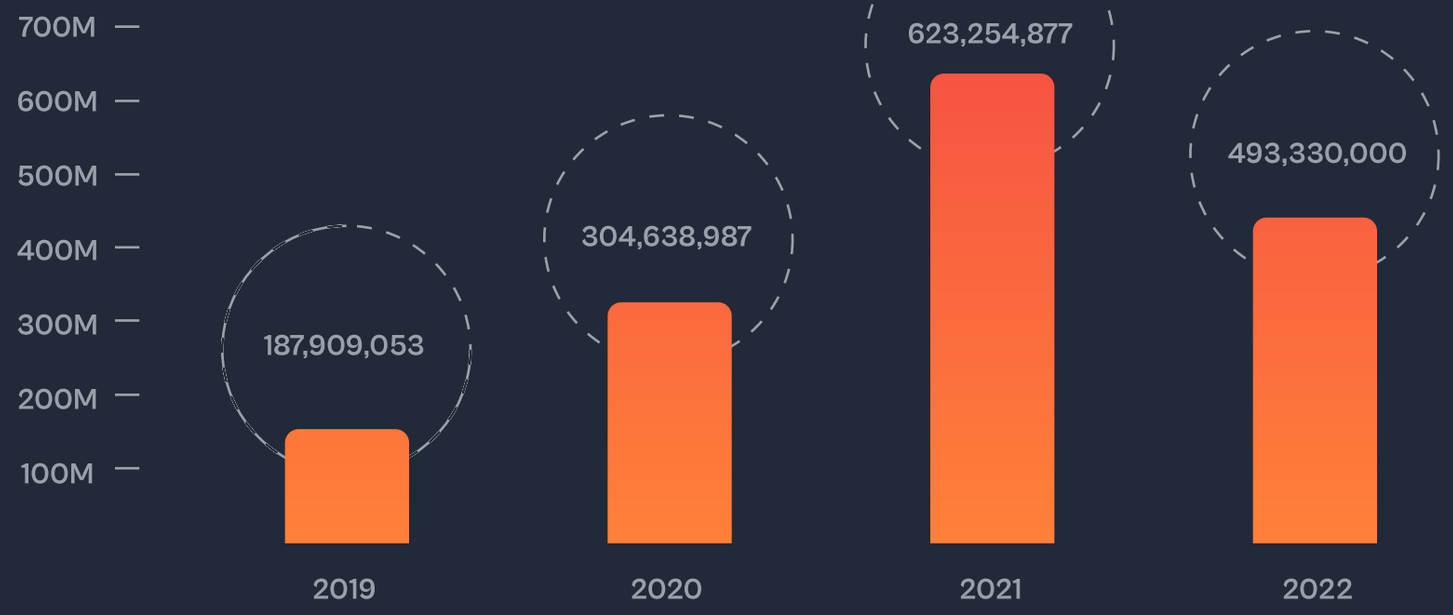
Average payment
$570,000

Additional Remediation Costs:
$1.85M

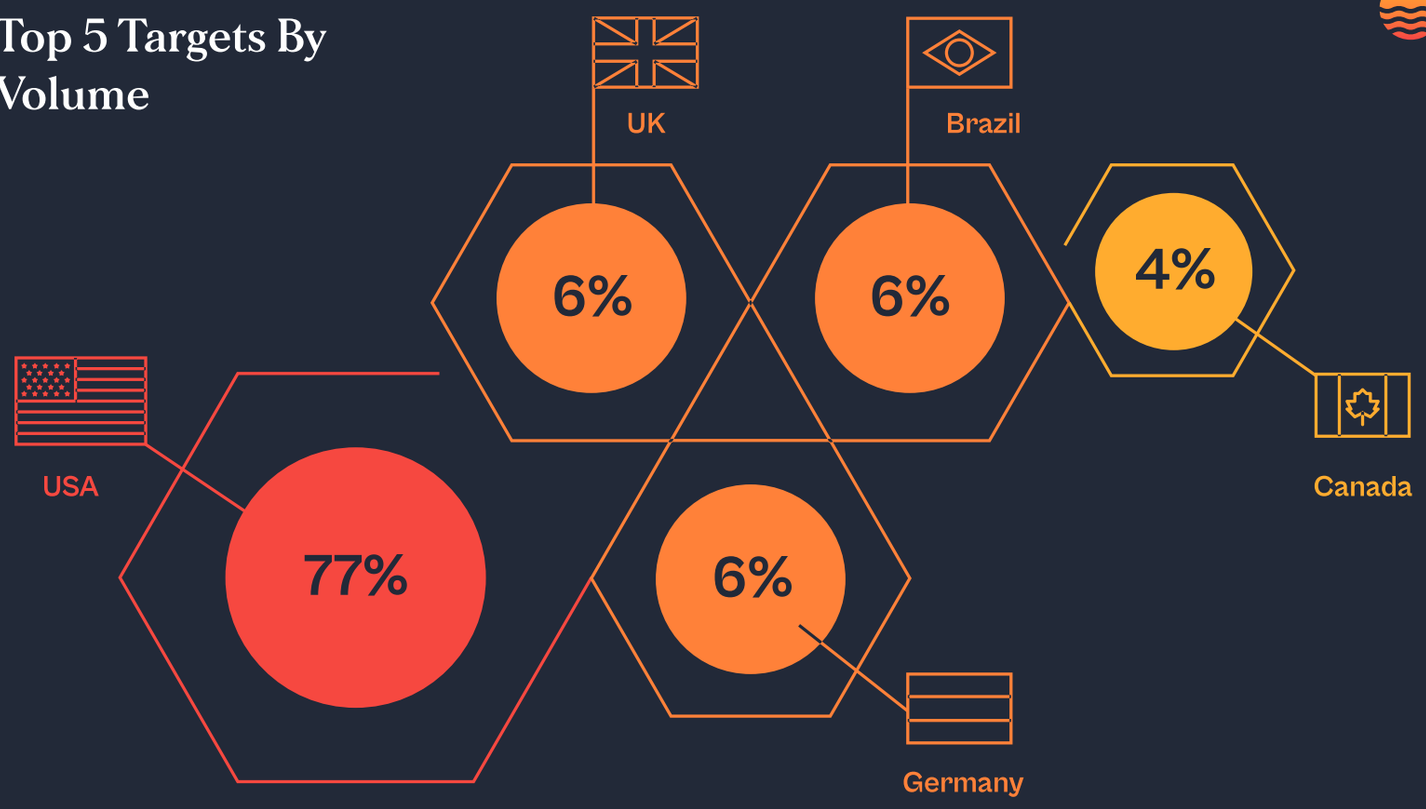
Targeted Orgs $100M+ Revenue
$100M+ Revenue

Ransomware Volume of Attacks

800M —

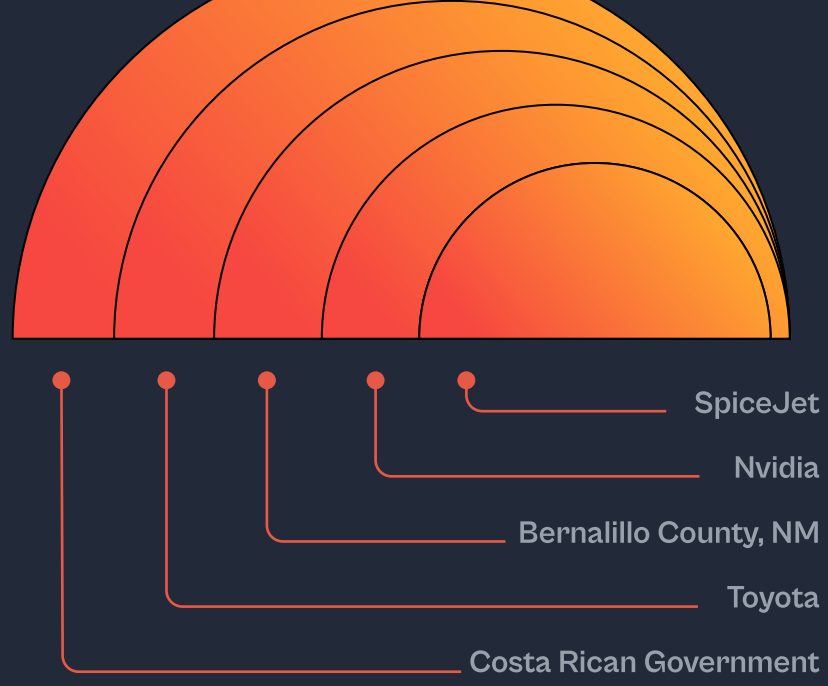


Top 5 Targets By Volume



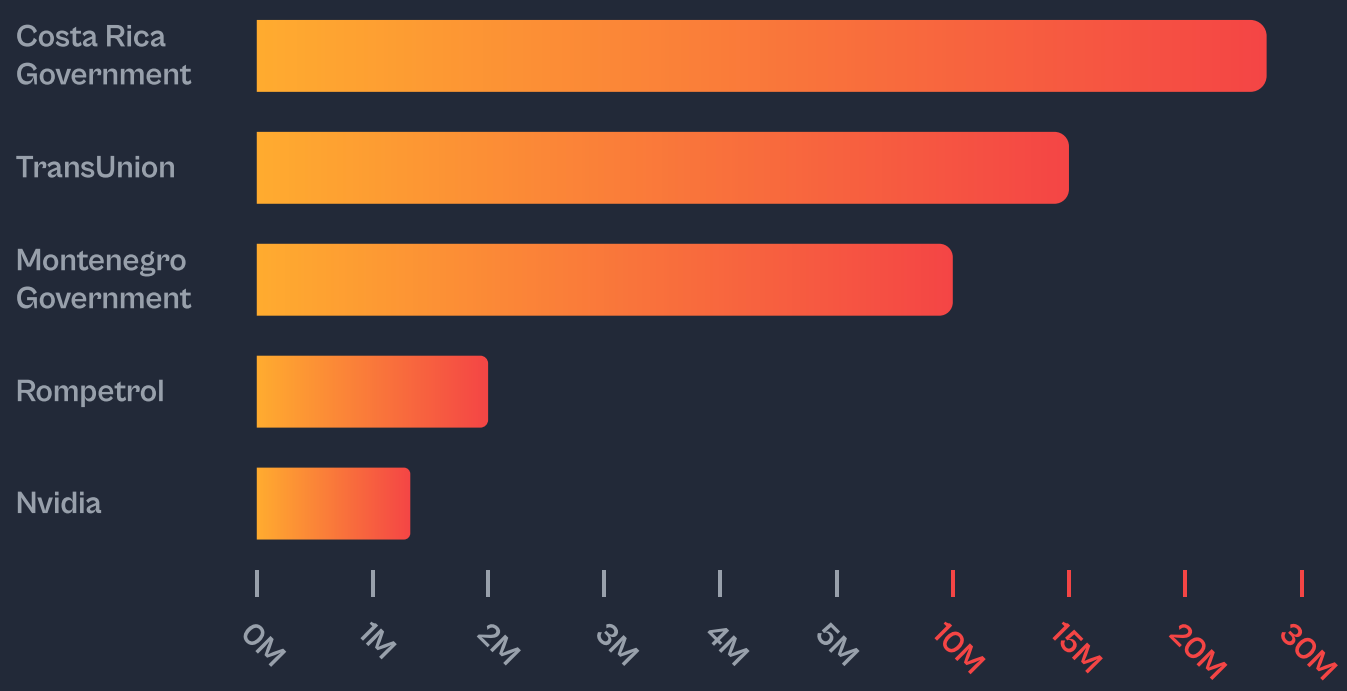
Most Disruptive Ransomware Attacks in 2022

Thousands of ransomware attacks occurring every week - here are just a few examples of some of the most disruptive attacks from 2022:

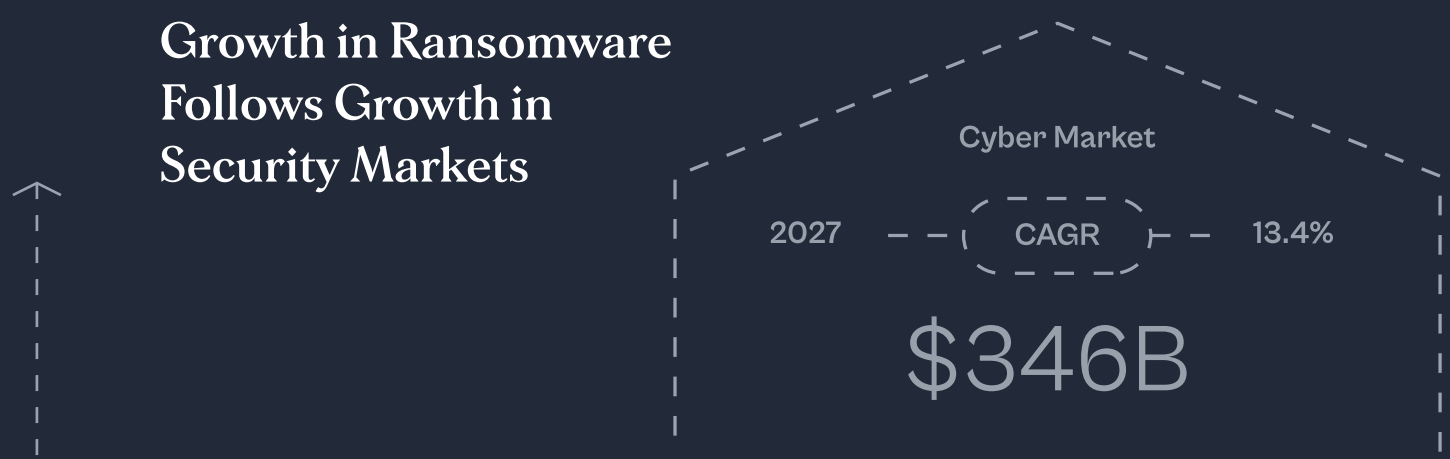


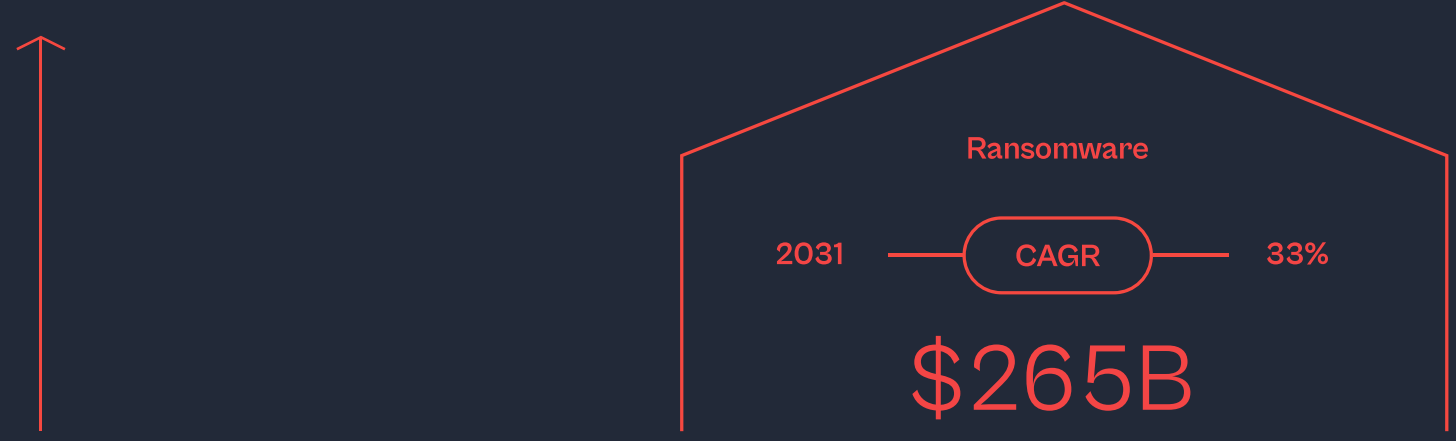
	Target	Impact
1	Costa Rican Government	$20 million ransom demand; healthcare system disrupted
2	Toyota	Operations at 14 plants disrupted; 5% reduction in production
3	Bernalillo County, NM	$2 million remediation; Metropolitan Detention Center disrupted
4	Nvidia	$1 million ransom demand; one terabyte of company data exfiltrated
5	SpiceJet	Data of 1.2 million customers compromised; flights delayed or cancelled

Top Reported Ransom Demands in 2022

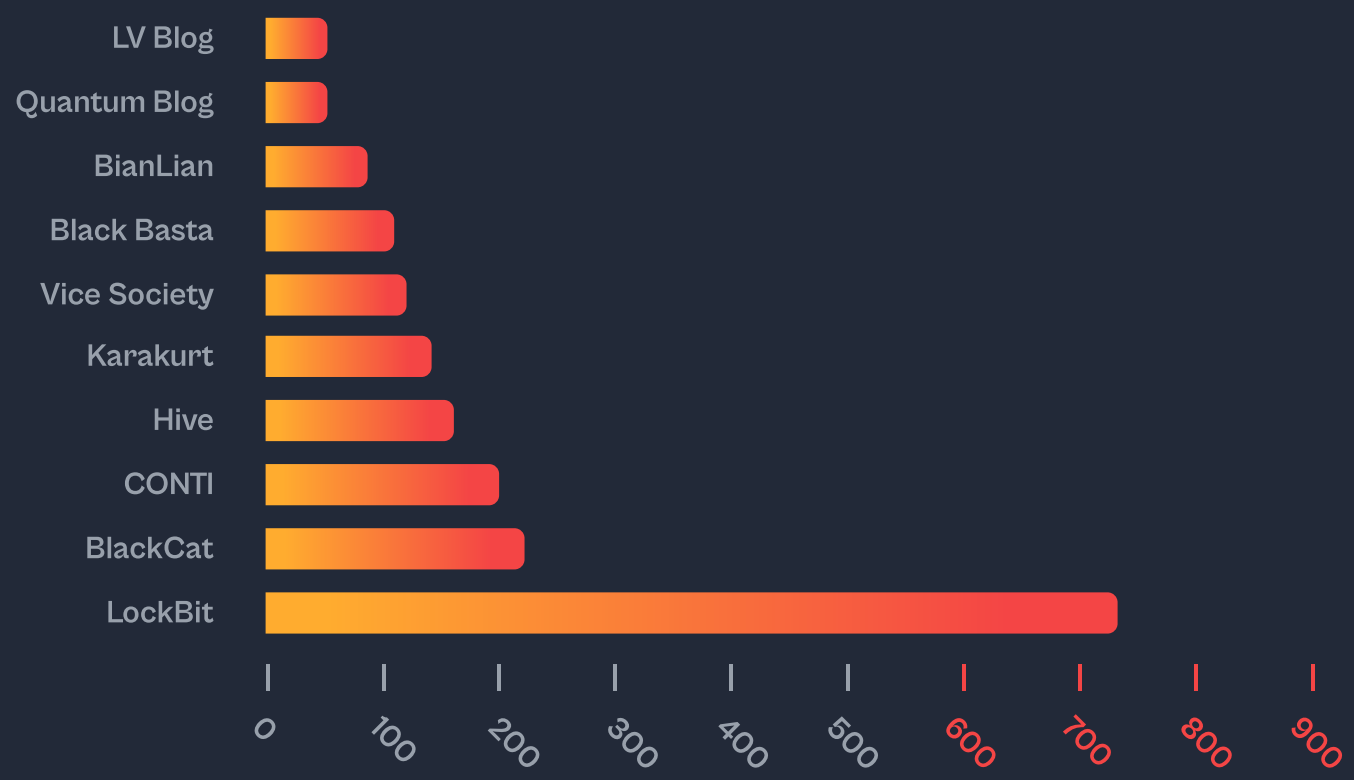


Growth in Ransomware Follows Growth in Security Markets





Total Victims Per Group in 2022 (Top 10)



The Halcyon Platform is Key to Resilience.

Threats like ransomware are designed to evade modern security tools, and just one miss can have a catastrophic impact on your organization. Halcyon is the first Anti-Ransomware and Cyber Resilience Platform with automated encryption key capture and autonomous decryption capabilities, to keep your operations running 24/7/365.

Learn more about Cyber Resilience and the Halcyon Platform by visiting halcyon.ai today

halcyon

halcyon.ai