CSNP
CYBERSECURITY NON-PROFIT

Ransomware Trends 2024 Report

A comprehensive analysis of ransomware attack patterns, trends, and defense strategies for 2024

CYBER SECURITY NON-PROFIT

ANNUAL REPORT

EXECUTIVE OVERVIEW

The Ransomware Landscape in 2024

Ransomware attacks have evolved into a multi-billion dollar criminal enterprise, with threat actors becoming increasingly sophisticated and brazen. This report analyzes key trends, attack patterns, and defensive strategies based on comprehensive data from 2024.

Key findings reveal a dramatic shift in attacker tactics, with double and triple extortion becoming the norm rather than the exception. Organizations across all sectors face unprecedented risks as ransomware groups leverage AI, automation, and supply chain vulnerabilities.

72%

Attack Increase

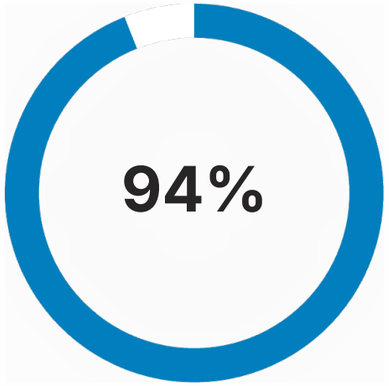
Year-over-year growth in ransomware incidents

$2.3M

Average Ransom

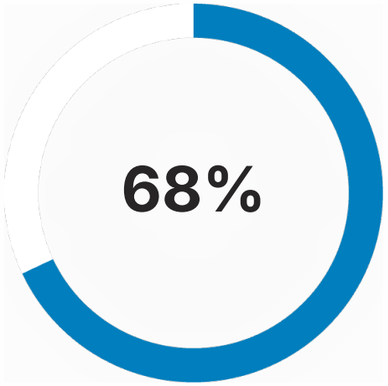
Median demand in 2024

Attack Frequency & Volume



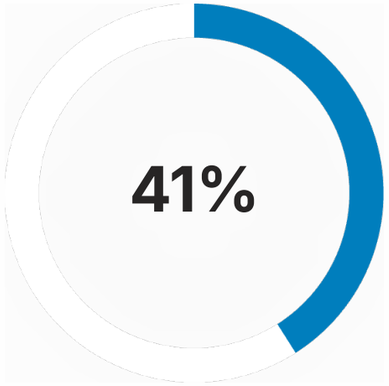
Organizations Targeted

Experienced at least one ransomware attempt in 2024



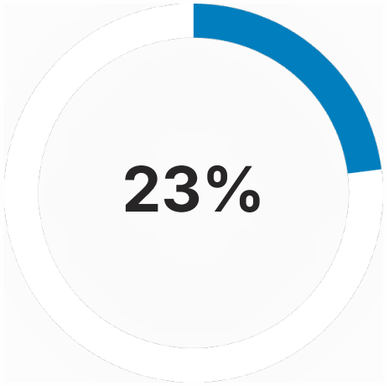
Successful Breaches

Of targeted organizations were successfully compromised



Multiple Attacks

Victims experienced repeated ransomware incidents



Data Exfiltration

Cases involved sensitive data theft before encryption

Attack volumes reached record highs in Q2 and Q3 2024, with threat actors launching coordinated campaigns targeting vulnerable infrastructure during peak business periods and holiday seasons.

Primary Attack Vectors

Understanding how ransomware enters your environment is critical for building effective defenses. These five vectors account for 94% of all successful ransomware deployments in 2024.

1

Phishing & Social Engineering

45% of attacks begin with compromised credentials obtained through sophisticated phishing campaigns, targeting employees with realistic impersonation and urgency tactics.

2

Unpatched Vulnerabilities

28% exploit known software vulnerabilities, particularly in VPNs, remote desktop protocols, and enterprise applications with delayed patch deployment.

3

Compromised Remote Access

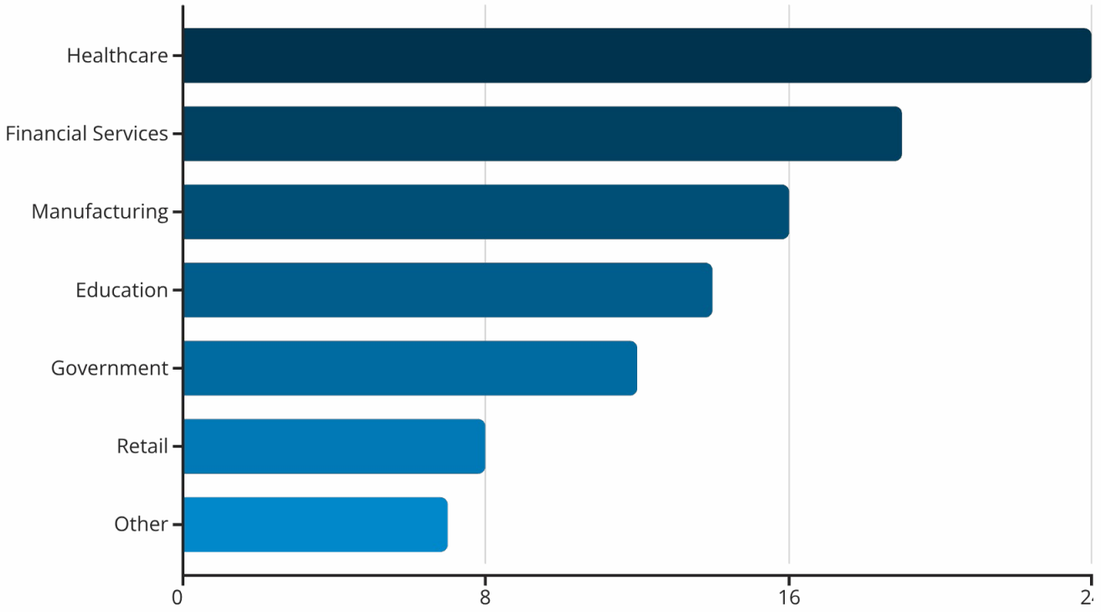
12% leverage stolen VPN credentials or poorly secured RDP endpoints, often purchased on dark web marketplaces from previous breaches.

4

Supply Chain Infiltration

9% penetrate through trusted third-party vendors, exploiting vendor management software and service provider access to multiple organizations simultaneously.

Industries Under Siege



Healthcare remains the most targeted sector due to critical patient care dependencies and valuable medical records. Financial services face attacks seeking transaction data and cryptocurrency wallets.

Manufacturing experienced the largest year-over-year increase, with attackers exploiting operational technology vulnerabilities and just-in-time production pressures to maximize ransom payment likelihood.

FINANCIAL IMPACT

The True Cost of Ransomware

Direct Ransom Payments

Average: $2.3M

Median demand increased 47% from 2023, with some enterprise attacks exceeding $50M

Recovery & Downtime

Average: $4.7M

System restoration, lost productivity, and business interruption costs often exceed ransom amounts

Long-Term Impact

Average: $3.2M

Reputational damage, regulatory fines, legal fees, and customer attrition create lasting financial burden

Total Average Cost: Organizations face an average total impact of **$10.2 million** per successful ransomware attack when accounting for all direct and indirect costs.

Evolution of Extortion Tactics

Single Extortion (Legacy)

Traditional encryption-only attacks demanding payment for decryption keys. Largely obsolete as organizations improved backup strategies.

Double Extortion (Standard)

Data theft before encryption, threatening public leak if ransom unpaid. Now the baseline approach for 87% of ransomware groups.

Triple Extortion (Emerging)

Adding DDoS attacks, customer notification threats, and direct victim contact. 34% of attacks in 2024 employed triple extortion tactics.

Quadruple Extortion (New)

Targeting business partners, supply chain pressure, and regulatory reporting threats. Rapidly growing sophistication increases pressure exponentially.

Ransomware-as-a-Service Ecosystem

The ransomware landscape has professionalized into a service-based economy, lowering barriers to entry and enabling less technical criminals to launch sophisticated attacks.

</>

Malware Developers

Create and maintain ransomware platforms, typically taking 20-30% of ransom payments

Affiliate Networks

Deploy attacks using provided tools, receiving 70-80% of proceeds

Initial Access Brokers

Sell compromised credentials and network access on dark web markets

Negotiation Services

Professional intermediaries handle victim communications and payment processing

Defense Strategy Framework

A comprehensive, layered approach is essential for ransomware resilience. These five pillars form the foundation of effective protection.

Prevention

- Multi-factor authentication everywhere
- Zero-trust architecture implementation
- Regular security awareness training
- Email filtering and web protection

Detection

- 24/7 security monitoring and SIEM
- Endpoint detection and response (EDR)
- Network traffic analysis
- Behavioral anomaly detection

Response

- Documented incident response plan
- Regular tabletop exercises
- Isolation and containment procedures
- Communication protocols

Recovery

- Immutable backup solutions
- Offline backup copies (3-2-1 rule)
- Tested restoration procedures
- Business continuity planning

Improvement

- Regular vulnerability assessments
- Patch management program
- Post-incident reviews
- Security metrics and KPIs

Actionable Recommendations

Immediate Actions (This Week)

- Enable MFA on all administrative and remote access accounts
- Verify backup integrity and test restoration process
- Review and update incident response contact list
- Disable unnecessary RDP and remote access ports

Short-Term Priorities (30 Days)

- Deploy EDR solutions on all endpoints
- Conduct ransomware-focused security awareness training
- Implement network segmentation for critical systems
- Review and patch critical vulnerabilities

Long-Term Strategy (90 Days)

- Develop comprehensive security roadmap
- Establish zero-trust architecture framework
- Implement security orchestration and automation
- Build threat intelligence program

Looking Ahead: 2025 Predictions

AI-Powered Attacks

Expect sophisticated AI-driven phishing, automated vulnerability exploitation, and adaptive malware that evades traditional detection methods.

Cloud Infrastructure Targeting

Increasing focus on cloud misconfigurations, SaaS application vulnerabilities, and multi-tenant environment exploitation.

OT/IoT Convergence Risks

Operational technology and IoT devices become primary targets as IT/OT convergence creates new attack surfaces.

Organizations must proactively adapt defenses to address emerging threats. Investment in AI-powered security tools, cloud security posture management, and OT security will be critical for maintaining resilience in 2025.

About Cyber Security Non-Profit

> *"Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."*

Our Free Programs

- **Business & Non-Profit Security** – Enterprise-grade guidance for organizations of all sizes
- **Family Cybersecurity** – Protecting your household in the digital age
- **Kids Safety** – Age-appropriate online safety education
- **Senior Digital Safety** – Empowering older adults against digital threats
- **Women's Security** – Addressing unique digital safety challenges
- **Parents & Educators** – Tools to protect and teach the next generation

Visit csnp.org | Access Free Resources